PCT/GB04/003537

GB04/3537

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

REC'D 10 SEP 2004
WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed Stephen Hurdley

Dated 25 August 2004

Patents Form 1/77

30MAR04 E884787-1 D10076
P01/7700 0.00-0407042.1 NONE

Patents Act 1977
(Rule 16)

THE PATENT OFFICE
K
29 MAR 2004
LONDON

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — 600689PGB

2. Patent application number *(The Patent Office will fill in this part in)* — 0407042.1

29 MAR 2004

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Serverside Graphics Limited
18 Maddox Street
London W1S 1PL
United Kingdom

Patents ADP number *(if you know it)* 08390940001

If the applicant is a corporate body, give the country/state of its incorporation — United Kingdom

4. Title of the invention — SECURE PRODUCTION FACILITY

5. Name of your agent *(if you have one)*

McDermott, Will & Emery
7 Bishopsgate
London EC2N 3AR

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Patents ADP number *(if you know it)* ~~0780510001~~ 08354469 0001

6. Priority: Complete this section if you are declaring priority from one or more earlier patent applications, filed in the last 12 months

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. Divisionals, etc: Complete this section only if this application is a divisional application or resulted from an entitlement dispute (see note f)

Number of earlier UK application	Date of filing *(day / month / year)*

8. Is a Patents Form 7/77 (Statement of inventorship and of right to grant of a patent) required in support of this request — YES

Answer 'Yes' if:
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
Otherwise answer NO (See note (d))

Patents Form 1/77

9. Accompanying documents: A patent application must include a description of the invention. Not counting duplicates, please enter the number of pages of each item accompanying this form:

Continuation sheets of this form	
Description	33
Claim(s)	0
Abstract	0
Drawing(s)	21 +21 R1

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for a preliminary examination and Search *(Patents Form 9/77)*	
Request for substantive examination (Patents Form 10/77)	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature(s) Justin Hill Date 29 March 2004

12. Name, daytime telephone number and email address, if any, of person to contact in the United Kingdom

Justin Hill - 020 7577 6943 - juhill@europe.mwe.com

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered YES in part 8, a Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) Part 7 should only be completed when a divisional application is being made under section 15(4), or when an application is being made under section 8(3), 12(6) or 37(4) following an entitlement dispute. By completing part 7 you are requesting that this application takes the same filing date as an earlier UK application. If you want a new application to have the same priority date(s) as the earlier UK application, you should also complete part 6 with priority details.

Secure Production Facility

The charts on drawing pages 1 through 7 show methods of securely reconciling a customer's design with their information so that the design ends up being applied to a product with the relevant customer information. Page references hereinafter refer to pages of these drawings. The example given is again the production of a financial transaction card in which the customers design must be reconciled with the customers financial information during the card fabrication process.

Essentially, all the systems have the financial information passing down a secure network (shown by the dotted line). In no cases does this information pass to Serverside Graphics (in this case an application service provider).

In all cases Serverside Graphics is passed an ID which is unique to the cardholder but that cannot be traced back to the cardholder by a third party.

In the charts showing the use of a MD5 Hash some of the cardholder information is encrypted using a one-way encryption technology at both the beginning and end of the cycle enabling the IDs to be reconciled. I believe this has been covered in previous applications.

The system used to date is represented in page 3 As you can see the vast majority of the work is done at the card personalisation plant. This has a couple of important disadvantages:

1. There needs to be a printer at every plant (cost +/- £180,000)
2. The card has already got the hologram and some logos on and thus there are registration / tolerance issues to print up to these elements
3. The printer can not print gold / UV / Pantone compliant colours
4. The Quality is not sufficient to lay down the Card association marks
5. Each card costs US$.25 to print.
6. All of the images need to be sent to the card production facility which is difficult to do for multiple deployments.
7. Re-issue in the event of loss is difficult for the issuer – they need to warehouse all the images and pull old images for re-issue on one system whilst combining with new cards to be printed for that day.

The present application seeks to provide improvements. For example, the charts involving the HP in particular are new (see pages 4, 5, 6 & 7).

These methods and apparatus enable the cards to be printed at the card manufacturer on a huge digital printer designed for printing large volumes of cards but able to put a unique image on each.

The limitation is that the machine print in sheets and then the cards are cut free. There are 4 visible colours and 2 others – one prints UV and the other could be metallic, fluorescent or similar. But preferably they're all ink.

So we can embed a code in the digital image to be printed. This can be as text, barcode, microdot, microtext and several other methods. Essentially, it is not believed the way it is written to be material – all are writing a code / identifier to be read later and enable the cards to be reconciled with their financial information in a secure fashion.

The Read / Write module is a box that reads the optical ID in the ink layer and writes it to another medium (probably the magnetic stripe in the real world) that can be easily read by a card personalisation module to pull the emboss record for the individual and enable the embossing to be added to the card and for it to be mailed to the correct recipient.

In the real world it might be preferable to put the code down in two formats so that the code can be read in the event of a miss-scan.

The advantages are:

- Cheap
- Extremely easy for the issuer – very few changes to current systems
- Can personalise the entire card, right up to the issuer logos and the hologram
- Can print at 800 dpi
- Pantone compliant – can print logos dependably
- Since the printer will frequently supply to many issuers it is cost effective to have a dedicated internet pipe from our site to the print facility
- Easier to re-issue cards in event of loss (simply send DID of old card to us along with DIDs of new issues and the rest just happens)

Notes on Printers and equipment.

There are four main pieces of machinery utilised in the charts. These are have been given the names "Artista", "HP" and "9000" which relate to current market-leading products of each type and "read /write". Other competitive products could be used at each stage.

9000

"9000" is a card personalisation machine which can be modular. Typically it has components that emboss a card, add tipping encode the magnetic stripe and combine the card with a pre-addressed letter or envelope for mailing.

Components could also include an magnetic stripe reader, a bar-code reader and other optical readers in future.

Artista

A card printer which lays an image onto a card at the time of personalisation. It is not currently in-line with other personalisation machines but could be in the future.

"Artista" prints onto a blank card (or a card with blank areas) by pulling an image from a local image server where the images are kept alongside their financial information. The Artista both lays down the digital image on the card and simultaneously encodes the magnetic stripe on the back of the card.

The "9000" can now read the magnetic stripe on the back of the card and use this to get the remaining cardholder information in order to emboss, and prepare the card for mailing.

HP

This is a high quality commercial digital press designed to digitally print financial cards. Typically this press will be pantone compliant and print at over 800 dpi. These can lay down logos, brand marks, optical ids and card designs in a single process both rapidly and economically. Every card can be printed with different information.

Read/ write

The "Read / Write" module is a box that reads a code in the ink laid down by the HP and writes it to another medium (probably the magnetic stripe) that can be easily read by a "9000" card personalisation module to pull the emboss record for the individual and enable the embossing to be added to the card and for it to be mailed to the correct recipient.

Chart on page 2

Product without personalisation.

This chart is by way of reference, it shows the processes utilised by a card issuer using a Digital Card printer to produce non-personalised card. As can be seen the Card manufacturer does not receive any financial information – this is passed securely down the network described by the dotted line (**4**).

Nonetheless, the printed cards passed from the Card Manufacturer to the Card Personalisation facility do so securely (in a security van or similar).

Chart on Page 3

Production using Artista and ID passed with emboss file.

This is a first Serverside Graphics process. It shows a blank stock card being passed (**6**) to the personalisation facility. At this point, an image is applied to it.

The DID which is passed to the SSG hosting facility (**1**) is a unique, non-sequential ID that has no other significance other than as a tie between the image to be created and the individual that is designing the card.

At point (**2**), the DID is passed back to the issuer as confirmation that a design has been successfully completed.

The digital images, along with their ID are passed to the Card Production facility (**3**).

The DIDs are passed along with the financial information securely to the card personalisation facility (**4**).

Issues with this deployment:

- As can be seen in (**5**) there is much extra work at the card personalisation facility.
- The images required for printing are called locally – requiring them to be stored locally at the personalisation facility.
- Although the print quality is high there are registration issued between the elements laid down in the first print job and the second.
- There are many personalisation facilities that run only small numbers of cards.
- There is extra print equipment at every personalisation facility – which requires extra staff training.
- The print equipment (Artista) is costly (US$ 250,000) and is held at every personalisation facility. Thus it is difficult to use it to its maximum economic potential.

- The printer has a high consumable cost per card (US$.25 each)
- Images need to be transferred to every personalisation facility, which is difficult and costly to do reliably and securely.

Chart on Page 4

Production using HP and ID passed with emboss file.

This diagram shows how personalisation can be made possible at the Card manufacturer's facility in a secure fashion.

The DID which is passed to the SSG hosting facility (**1**) is a unique, non-sequential ID that has no other significance other than as a tie between the image to be created and the individual that is designing the card.

At point (**2**), the DID is passed back to the issuer as confirmation that a design has been successfully completed.

In (**3**), the issuer passes back to Serverside Graphics the DIDs that have both completed their design and been credit approved. To this file can be added the DIDs of any cards that need re-issuing due to loss, expiry or similar.

As can be seen at (**4**), the successful DIDs are added to the information passed to the card personalisation facility.

At point **A** the DID is converted into an optical format (barcode, microdot, invisible ink etc) and is made into part of the digital image to be printed).

In (**5**) the list of DIDs to be issued is used to pull the relevant images from the image warehouse where they are stored.

In this exemplary process, the images alone are passed to the Serverside Graphics print server at the card manufacturers facility.

The Digital printer (HP) simply prints all the cards that are passed to it by the SSG print server (**6**)

At point **B** the Read / Write machine reads the optical image embedded at point A and converts it back to a digital ID. This ID can now be written back on the card magnetic stripe – which makes it readable to 9000 equipment.

The card is now passed through the conventional channel to the personalisation facility where the magnetic stripe is read and used to reconcile the card with its financial information.

Advantages of this method are:

- There is no additional equipment required at the card personalisation facility
- The print cost is very low – the increase in print cost is nil or very low
- Since there is only one print process the elements can be printed right up against each other
- The print quality is very high indeed (800 dpi versus 300 dpi for Artista)
- Neither the issuer nor the personalisation facility needs to deal with cumbersome digital images
- Images are passed in large volumes to a small number of printers and between two boxes of Serverside Graphics' design. This enables a fast dedicated line to be put in place.
- Only images are passed to the Card Manufacturer – this means that the DID (although secure) does not need to be passed and only one file type needs to be passed in one direction which is easy to lock down in a firewall.
- It is very simple for a card issuer to request a card to be re-issued – they simply send the same list of DIDs to Serverside at (**3**) as they send to the personalisation facility at (**4**)
- There is very little change in process at the either Card Manufacturers facility
- Processes at the Card Personalisation facility are entirely in-line.

Chart on Page 5

Production using HP and one-way encryption ID

This process is very similar to the process shown on page 4; it differs at points **C**, **D** and (**4**). The major difference is felt at (**4**), at this point, only financial information is passed between the issuer and the personalisation facility. This is identical to the process shown at (**4**) on page 2.

The method by which the ID is removed from this process is by running identical encryptions on some unique information held in the financial details passed between the issuer and the personalisation facility. This encryption is carried out by the encryption modules at **C** & **D**. Since the same encryption is run, using the same algorithms, on the same information at both of these points the same final result will be produced. This result is used as the DID to be carried with the card.

The Card is duly reconciled with it's financial information at the card personalisation facility

This method has most of the advantages of the chart on page 4 and the additional benefit that:

- No DID needs to be passed down the secure network along with the Financial information. This means that legacy IT systems do not need to be adjusted.

Chart on Page 6

Production using HP and ID passed with emboss file using Optical ID compatible with 9000

This process is very similar to the process shown on page 4; it differs at points **E** and **F**.

Essentially, the difference here is that there is no Read/ Write machine at the card production facility (**E**). The Optical ID that is embedded in the image to be printed on the card is readable by a machine resident at the card production facility (**F**).

This method has most of the advantages of the chart on page 4 and the additional benefit that:

- No additional equipment is required at the Card Manufacturer's facility.
- Processes at the Card Personalisation facility are still in-line

There is a possible disadvantage however in that the size and type of Optical ID to be used is dependant on the equipment at the personalisation facility and this may lead to large or unsightly marks on the card or to the card being refused at point of sale – all of which are unacceptable to both the card issuers and the governing card associations.

Chart on Page 7

Production using HP and one-way encryption using Optical ID compatible with DC9000

This chart shows each of the advances on the chart on page 4 made in pages 5 and 6 combined. The points of each of the advances are shown at points **C,** (**4**), **D, E** and **F.**

This method has most of the advantages of the chart on page 4 and the additional benefits that:

- No additional equipment is required at the Card Manufacturer's facility.
- Processes at the Card Personalisation facility are still in-line
- No DID needs to be passed down the secure network along with the Financial information. This means that legacy IT systems do not need to be adjusted.

There is a possible disadvantage however in that the size and type of Optical ID to be used is dependant on the equipment at the personalisation facility and this may lead to large or unsightly marks on the card or to the card being refused at point of sale – all of which are unacceptable to both the card issuers and the governing card associations.

Further disclosure and information is provided on the attached Annex.

Annex

" Apparatus and Method for Manipulating Images"

APPARATUS AND METHOD FOR MANIPULATING IMAGES

TECHNICAL FIELD

This invention relates to methods and apparatus for manipulating images; and in particular to methods and apparatus for reproducing personalized images on consumer goods at locations remote from a user. The preferred embodiment includes on-line product-based image manipulation software.

BACKGROUND

There has been an increasing consumer desire for self-differentiation, particularly for differentiating mass-marketed personal items. This can be clearly seen in the recent popularity of customized mobile phone ring-tones and fascias. In order to provide personalized graphics on consumer products, there has therefore been a need for a quick and easy-to-use graphics manipulation suite to allow users to make product-specific designs, particularly from locations remote from the main image storage and printing facility. However, providing such a graphics manipulation suite over the Internet has not proved easy.

One problem stems from the open nature of the Internet itself. In order to allow Internet users to visit hundreds of thousands of unverified web sites, and yet still protect the user's computer from viruses and malicious hackers, a browser must not allow the web sites to access files on the user's computer. Thus, browsers are "dummy terminals," albeit very powerful ones; it is not easy to actively "do" anything with an Internet browser – it simply navigates between online resources and presents information and images to the user. Thus, for designing a graphical image for application to a personal item, an internet user may be able to manipulate

images within the browser environment, but will not be able to save the images.

The problem of manipulating images to be applied to an article remote from the user has previously been solved in two ways, each of which has disadvantages. In one solution, a user manipulates images on his or her own machine without the use of a browser. This solution has the advantage of being extremely fast once installed on the local machine, but suffers from three major failings. First, in order to allow the program to run on the client machine, the user must first download a program. This takes time, and is inconvenient, because the software cannot be seen or tested until it is fully downloaded. Next, the program must be installed on the user's machine, where it will remain permanently until removed. This occupies storage space on the client hard drive, slows down the user's computer, and can cause system crashes. Finally, the downloaded program may have computer viruses.

In another image manipulation solution, an image is manipulated directly on a server using Java Applets, or another plug-in that functions in a similar fashion, such as a custom Activex control. Each time the user uses the interface to make a manipulation to the image, a separate call is made to the server; the server software changes the image's position, and sends back the information to the client machine. The theoretical advantages of Java and similar programs are that they can run on any client machine with identical results; and that the software does not need to be installed on the client machine, because the Java Applet runs within a Java Virtual Machine of the browser. However, the problem with Java and similar programs is that the Internet simply is not fast enough to provide a pleasant user experience. Also, in practice, because the Java Applet does not know which type of machine it will be run on, it can react very differently from one machine to the next.

SUMMARY

In one embodiment according to the invention, there is disclosed a computer system for manipulation of remote images. The computer system comprises: a browser-based user interface for displaying for manipulation a graphical representation of at least a portion of an image held at a remote image store; an internet communications link coupling the user interface to a remote image processor, said link being operable to transfer information about manipulations applied to the graphical representation between the user interface and the remote image processor; and means for the remote image processor to access the remote image store in order to apply to the

image held in the store manipulations emulating those applied to the graphical representation.

In related embodiments, the image held at the remote image store may be of a relatively higher resolution than the graphical representation of at least a portion of the image. The remote image processor may further comprise means for communicating a version of the image, comprising the applied manipulations, to an image printing means maintained securely from the user interface. The computer system may further comprise means for associating a unique identifier with a user applying the manipulations to the graphical representation; wherein the internet communications link is operable to transfer the unique identifier between the user interface and the remote image processor. The remote image processor may also comprise means for receiving a hash value, which relates to a user who applied the manipulations to the graphical representation. The browser-based user interface may be presented on a kiosk accessible to a consumer. The kiosk may comprise a printer for printing an image, produced by applying the manipulations that emulate those applied to the graphical representation, onto a consumer item. The computer system may also further comprise a database capable of storing the information about the manipulations applied to the graphical representation; such that a manipulation can be applied to the image held in the remote image store, other than in real time, or alternatively, allowing printing tasks to different articles to be batched. The computer system may further comprise a printer for printing an image, produced by applying the manipulations that emulate those applied to the graphical representation, onto a consumer item. The consumer item may comprise a financial account access means.

In another embodiment according to the invention, there is disclosed a method of operating a computer system for manipulation of remote images. The method comprises: displaying for manipulation at a browser-based user interface a graphical representation of at least a portion of an image held at a remote image store; providing an internet communications link coupling the user interface to a remote image processor; transferring information about manipulations applied to the graphical representation between the user interface and the remote image processor; and causing the remote image processor to access the remote image store and to apply, to at least a portion of the image held in the store, manipulations emulating those applied to the graphical representation.

In related embodiments, the method may further comprise transferring a unique identifier between the user interface and the remote image processor, the unique identifier being associated

with a user applying the manipulations to the graphical representation. The method may also comprise receiving a hash value at the remote image processor, the hash value relating to a user applying the manipulations to the graphical representation; or presenting the browser-based user interface on a kiosk accessible to a consumer. A printer at the kiosk may be used to print an image, produced by applying the manipulations that emulate those applied to the graphical representation, onto a consumer item. The method may also further comprise storing information about the manipulations applied to the graphical representation in a database, such that the manipulations can be applied to the image held in the remote image store, other than in real time, or alternatively, allowing printing tasks to different articles to be batched. The method may also comprise printing an image, produced by applying the manipulations that emulate those applied to the graphical representation, onto a consumer item, which may comprise a financial account access means.

In another embodiment according to the invention, there is disclosed a computer program product comprising program code means, said program code means including: first code means for displaying for manipulation at a browser-based user interface one or more graphical representations of at least a portion of an image held at a remote image store; second code means for establishing an internet communications link coupling the user interface to a remote image processor; third code means for transferring information about manipulations applied to the graphical representation between the user interface and the remote image processor; and fourth code means for causing the remote image processor to access the remote image store and to apply to at least a portion of the image held in the store manipulations emulating those applied to the graphical representation.

In a further embodiment according to the invention, there is disclosed a computer system for manipulation of remote images. The computer system comprises: a front end server system for operating computer program means for providing a user interface for displaying a graphical representation of at least a portion of an image held at a remote image store for user selection from amongst a plurality of similar such graphical representations of at least a portion of each of a plurality of images held at the remote image store; and an internet communications link coupling the front end server system to a remote image processor capable of accessing the remote image store in order to select the original image held in the store, from amongst the plurality of similar such images held in the store, in a corresponding fashion to the user selection made on the

user interface.

In a related embodiment, the computer program means may further comprise means for enabling user manipulation of the graphical representation on the user interface; and the remote image processor may comprise means for accessing the remote image store in order to apply to the image held in the store manipulations emulating the user manipulations of the graphical representation on the user interface.

In another embodiment according to the invention, there is disclosed a system for applying a personalized image to a financial account access means corresponding to a financial account of a customer. The system comprises: a financial account association table associating financial data, corresponding to the financial account of the customer, with a customer identifier; an image manipulation emulator for associating the customer identifier with user image selection data based on user selections made on a user interface in relation to a graphical representation of at least a portion of an original image held in an image store; and an image application means for applying the personalized image to the financial account access means, the personalized image being based on the user image selection data associated with the customer identifier by the image manipulation emulator; wherein the system maintains at least the financial account association table securely from the user interface.

In further related embodiments, the system may further comprise a front end server for presenting the user interface; and a back end server, comprising the image manipulation emulator, for communicating with the front end server and with the image store. The front end server may further comprise means for communicating a user manipulation data string to the back end server. The financial account access means may comprise a credit card, debit card, or other transaction card means. The graphical representation of the original image may comprise a re-sized version of the original image. The original image may be uploaded from the customer's own computer. The user selections may comprise operations selected from rotating, re-sizing, positioning, flipping, controlling brightness, performing red-eye reduction, and adjusting opacity levels. The user selection data may further comprise data relating to at least one image for overlaying onto the original image; and the data relating to the at least one image for overlaying onto the original image may comprise at least one transparent portion. The user selections may also comprise operations for positioning at least a portion of the original image within a window region of the financial account access means. The window region may exclude regions of the

financial account access means that display functional features of the financial account access means. The user selections may also comprise operations for positioning at least a portion of the original image in relation to a template of features of the financial account access means. The financial account access means may comprise one of a credit card, debit card, or other transaction card means; and the features of the financial account access means may comprise one or more of a bank logo, a transaction card hologram, and a transaction card type indicator.

In another embodiment according to the invention, there is disclosed a method for applying a personalized image to a financial account access means corresponding to a financial account of a customer. The method comprises: associating financial data, corresponding to the financial account of the customer, with a customer identifier in a financial account association table maintained securely from a user interface; associating the customer identifier with user image selection data based on user selections made on the user interface in relation to a graphical representation of at least a portion of an original image held in an image store; and applying the personalized image to the financial account access means, the personalized image being based on the user image selection data associated with the customer identifier.

In further related embodiments, the method further comprises presenting the user interface using a front end server; and using a back end server, in communication with the front end server and the image store, to re-create the user selections made on the user interface. The method may also further comprise communicating a user manipulation data string from the front end server to the back end server. The financial account access means may comprise a credit card, debit card, or other transaction card means. The graphical representation of the original image may comprise a re-sized version of the original image. The method may further comprise uploading the original image from the customer's own computer. The user selections may comprise operations selected from rotating, re-sizing, positioning, flipping, controlling brightness, performing red-eye reduction, and adjusting opacity levels. The user image selection data may further comprise data relating to at least one image for overlaying onto the original image, where the at least one image for overlaying may comprise at least one transparent portion. The user selections may comprise operations for positioning at least a portion of the original image within a window region of the financial account access means. The window region may exclude regions of the financial account access means that display functional features of the financial account access means. The user selections may comprise operations for positioning at

least a portion of the original image relative to a template relating to features of the financial account access means. The financial account access means may comprise a credit card, debit card, or other transaction card means; and the features of the financial account access means may comprise one or more of a bank logo, a transaction card hologram, and a transaction card type indicator.

In another embodiment according to the invention, there is disclosed a method of operating a computer system to apply a personalized image to a financial transaction card. The method comprises: providing a financial account association table associating financial data of a customer with a customer identifier; receiving at an image processor a set of manipulations applied to a representation of an image at a remote user terminal, to generate a personalized design; processing the represented image by applying the received set of manipulations to produce a personalized image; and sending the personalized image for application to a financial transaction card, provided with banking features based on at least the customer identifier.

In a further embodiment according to the invention, there is disclosed a computer system for controlling production of a personalized financial transaction card. The computer system comprises: a financial account association table associating financial data of a customer with a customer identifier; a communication interface arranged to receive a set of manipulations applied to a representation of an image at a remote user terminal to generate a personalized design; an image processor to process the represented image by applying said set of manipulations to produce a personalized image; and financial card production equipment capable of receiving the personalized image and relevant financial data based on the customer identifier to produce a personalized financial transaction card.

In another embodiment according to the invention, there is disclosed a method of operating a computer system to produce a personalized financial transaction card. The method comprises: receiving a unique one-way code generated within a secure environment from information relating to a customer account; receiving at an image processor an image, and manipulating the image in accordance with instructions from a remote terminal operated by said customer; storing the manipulated image in association with the one-way code; and providing said manipulated image for application to a financial transaction card, responsive to a request comprising an identical one-way code generated independently from said customer account information.

In a further embodiment according to the invention, there is disclosed a computer system for producing a personalized financial transaction card. The system comprises: an interface for receiving from a secure environment a unique one-way code generated from customer account information; an image processor operable to manipulate an image in accordance with instructions from a remote terminal operated by said customer; a data store for storing the manipulated image in association with the one-way code; and an interface operable to supply said manipulated image for application to a financial transaction card responsive to a request comprising an identical one-way code generated independently from said customer account information. The customer account information may comprise at least a portion of an embossing record.

In accordance with any of the preceding embodiments, a kiosk accessible to consumers may be provided for performing manipulations to the graphical representation and/or for producing financial transaction cards applied with a personalized image.

In another embodiment according to the invention, there is disclosed a computer system for producing personalized financial transaction cards. The computer system comprises: means for generating a browser-based user interface for displaying on a remote terminal a graphical representation of at least a portion of an image, said interface being capable of effecting a plurality of manipulations to the graphical representation; an internet communications link coupling the remote user interface to an image processor, said link being operable to receive instructions defining said plurality of manipulations applied to the graphical representation from the remote terminal; an image processor operable to access the image to apply manipulations emulating those applied to the graphical representation according to the instructions; and financial transaction card production equipment operable to apply the resulting image to a financial transaction card.

In a further embodiment according to the invention, there is disclosed a method of operating a computer system to produce a personalized financial transaction card. The method comprises: receiving encrypted customer information generated within a secure environment from information relating to an account of the customer; receiving at an image processor an image, and manipulating the image in accordance with instructions from a remote terminal operated by said customer; storing the manipulated image in association with the encrypted customer information; and providing said manipulated image for application to a financial transaction card, in association with the encrypted customer information, to an entity having an

encryption key capable of decrypting the encrypted customer information.

In another embodiment according to the invention, there is disclosed a method of operating a computer to facilitate production of a personalized financial transaction card. The method comprises: providing means for presenting to a remote customer a user interface; receiving instructions for manipulation of an image file, the instructions being based on manipulations performed by the remote customer with regard to a representative version, on the user interface, of the image that is contained in the file; and providing an image, produced based on said instructions for manipulation, for application to the financial transaction card, the image being associated with a customer identifier corresponding to the remote customer.

In further related embodiments, the customer identifier may comprise one of: a one-way code, a unique customer identifier, and encrypted customer information. The one-way code may be created by a card issuer applying a one-way code function to financial account information of the remote customer. The encrypted customer information may be encrypted by a card issuer encrypting financial account information of the remote customer. Providing the means for presenting the user interface may comprise operating a website server. The provided image for application to the financial transaction card may be provided to a card bureau. The customer identifier may be embedded in the image produced based on said instructions for manipulation; including by being embedded as a machine-readable code, as a bar code, or by being embedded in file metadata. In one embodiment, the image file is not transferred to the user interface.

In another embodiment according to the invention, there is disclosed a system for operating a computer to facilitate production of a personalized financial transaction card. The system comprises: computer program means for presenting to a remote customer a user interface; image instruction means for receiving instructions for manipulation of an image file, the instructions being based on manipulations performed by the remote customer with regard to a representative version, on the user interface, of the image that is contained in the file; and image processing means for providing an image, produced based on said instructions for manipulation, for application to the financial transaction card, the image being associated with a customer identifier corresponding to the remote customer.

In further related embodiments, the customer identifier may comprise one of: a one-way code, a unique customer identifier, and encrypted customer information. The customer identifier may comprise a one-way code created by a one-way code function applied to financial account

information of the remote customer. The customer identifier may also comprise encrypted customer information created from encrypted financial account information of the remote customer. The computer program means may comprise a web server application of a website server. The image processing means may comprise means for providing the image for application to the financial transaction card, to a card bureau. The image processing means may also comprise means for embedding the customer identifier in the image produced based on said instructions for manipulation; such as by using means for embedding the customer identifier as a machine-readable code, as a bar code, or as file metadata.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention, and to show how the same may be carried into effect, reference will now be made, by way of example only, to the accompanying drawings, in which:

Fig. 1 illustrates a computer system for remote manipulation of images, in accordance with an embodiment of the present invention;

Fig. 2 illustrates a method of operating a computer system for remote manipulation of images, in accordance with an embodiment of the present invention;

Figs. 3-10 show screens of a credit card design website, operated in accordance with an embodiment of the invention;

Fig. 11 illustrates a method of operating a computer system for remote manipulation of images, using a unique customer identifier, in accordance with an embodiment of the present invention;

Fig. 12 illustrates a method of operating a computer system for remote manipulation of images, using a hash value to avoid the need for creating and maintaining a unique customer identifier through the card application and printing lifecycle, in accordance with an embodiment of the present invention;

Fig. 13 illustrates a system according to an embodiment of the invention, in which an image is designed using a card-issuing kiosk or in-store instant issue system; and

Fig. 14 illustrates a system in which a database is used to store information between a user's image selections and back end image production, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

An embodiment according to the invention allows a user to manipulate an image through a browser interface, and is divided into two software portions, here referred to as front end software and back end software.

The front end software operates entirely within an Internet browser and in most cases does not require a download, because it accepts the limitations of the browser. In one embodiment, the front end software runs Flash software, available from Macromedia Inc. of 600 Townsend Street, San Francisco, CA 94103, U.S.A., or equivalent software. The front end software is a pure Graphical User Interface (GUI), and allows a user to design and edit graphics on his or her screen in order to build a representation of a desired image. Representations of stock (starting) images can be presented to a user in an on-screen image library and/or created by the user on demand. The image desired for output can be made up from one or several representative components, each of which has its position defined relative to an origin, and can be manipulated based on a set of predetermined rules - such as, for example, rules allowing the image or its components to be resized, rotated, flipped, mirrored and moved relative to other components. The representative graphical components can be used, for example, to build relatively complex designs consisting of a plurality of different layers and/or transparencies constructed using Flash scenes.

When the design is completed, in an embodiment according to the invention, instructions about what the final image looks like are sent to the back end software, which runs on a server. In the preferred embodiment, these instructions are sent together (simultaneously) after the manipulation is completed, and take the form of a text string for each component of the image. For example, the text string **makeimage.aspx** for a graphics component might read:

id+=030, x=182, y=32.3, flip=yes, rotate=270, scale=190.6, user=230

where **id** is an image identifier; **x** and **y** define the position of a component relative to a predetermined origin; **flip**, **rotate**, and **scale** define manipulations of types generally well known in the art; and **user** is a number identifying the user. Those of skill in the art will appreciate that a range of image manipulations can be defined in this way. A resulting image may be

represented by one or a number of graphical components. It is thus possible for a plurality of text strings, or an extended text string, to define an image made of a plurality of separate graphical components. The graphical components used, for example, in Flash movie scenes are generated and manipulated with a minimum of computing resources; and the designs constructed as a result can be recreated on the back end (server) side using the relevant (and generally much larger) image files. Relatively complex designs can be achieved by employing two or more image components with separate image identifiers. The image identifiers for graphical components of the same image may have a common characteristic. In accordance with embodiments of the invention, the instructions included in the text string that defines the manipulations needed to create the resultant image, need not all be included in a single text string; instead, a series of text strings may be transmitted separately to convey the same plurality of instructions. Furthermore, manipulations on the remote server need not await receipt of all of the series of text strings, but can instead be performed in stages as each string of the series is received. Regardless of the number of text strings used, an advantage of an embodiment according to the invention is that a smaller, emulated version of the image can be manipulated by the user with a minimum of computing resources, and instructions can be transferred efficiently as text strings; instead of requiring the inefficient (and time-consuming) transfer of large image files, or portions thereof, between the customer and an image-production server. Further, the need to make calls to a server with an image change each time that a single manipulation is made, is also overcome.

The back end software is responsible for generating the final image, in accordance with an embodiment of the invention, by interpreting the manipulations applied to the representation (defined in the, or each, text string file) and applying corresponding manipulations to one or more stock images held in a remote image store. The images used in the front end software are less computationally-demanding representations of those held on the server. As a result, the back end software can make image transformations that exactly mirror those which are seen on the client machine. Once the desired image has been created by the back end software, the image can be output to whatever device is required, such as a device for printing the image onto a personalized consumer item. In this way, the graphical representation is displayed and manipulated at the user interface by means of the Flash software, and only a minimal amount of information concerning the image and manipulations applied thereto need be transferred to the remote image processor.

As mentioned above, the front end software may use Macromedia's Flash, or another product. For example, the software could instead use HTML and Javascript (DHTML) without a download, although the GUI is relatively poor. Use of Flash (or equivalent) software is advantageous in that it does not allow full access to a user's local files, so that it does not risk transmitting computer viruses to the user's machine. Use of Flash software also does not require a user to install software other than the Flash plug-in, which has a high penetration of the browser market.

The preferred embodiment thus allows for on-line image manipulation by emulating the browser-based transformations (such as re-sizing or overlaying images), made by the user on a representation of the image, on the server so that the images produced can be used for personalised product creation.

On-line image manipulation is allowed by creating a two-tier architecture, in an embodiment according to the invention: there is one program that allows image manipulation on the screen in front of a user; and a second program on a server that emulates these manipulations, so that the images can be output for personalised product creation. In the preferred embodiment, the back end process, or elements of it, can be performed in a secure computing environment; and customised images can be printed onto an actual product under very high security (for example, bank level security). In this way, a user with internet access can design customised images for printing on a remote product which requires secure treatment, such as bank level security. For example, anti-fraud and anti-theft measures mean that the production of credit cards, and other types of transaction cards, is performed in secure locations. Customisation of the designs applied to such cards is thus possible, using preferred embodiments, without the need to give the user direct computing access to the secure environment.

An online image-editing tool uses the browser environment of HTML and Macromedia Flash as a Graphical User Interface for remote software that emulates the actions taken on the client machine, in an embodiment according to the invention. This enables a fast experience for the user and a high quality end product. However, the browser-based, client-side environment allowing manipulation by the user need not necessarily be Flash from Macromedia. Any equivalent software tool capable of providing the required functionality could be used - for example, any tool capable of generating a representation of an image, applying manipulations thereto, and transfering the results through a set of commands to the server-side software, such

that an image processor on the server side can emulate the actions of the front end and create a result image that can be saved to the server. The front end software will allow the upload of images from the user's computer to the server, so that the user's own images can be manipulated and overlaid with "stock" images and borders. Then, by communicating with the back end software, it is possible to produce personalized goods for a user. Such personalized goods may include, for example, credit cards, debit cards, mobile phone covers, mugs, T-shirts, gift cards, and framed prints.

An embodiment according to the invention has the advantage that high quality images do not need to be uploaded to the customer's browser during the manipulation process, because lightweight, web-enabled formats are instead used for the user's experience, thereby making the system fast and easy to use. However, when the information is transferred, the original high quality images are used to give high quality print results. An embodiment according to the invention also allows the provision of light-weight but fast graphics manipulation, without the complication of downloading programs. Additionally, a user interface according to the invention is not constantly calling to the server; thus the interface is quick and pleasant to use, and Internet bandwidth is used efficiently. As another advantage of an embodiment of the invention, the original image is not transferred over the internet at the manipulation stage, so that the possibilities for hacking the image are greatly reduced. Also, because the interface runs within the Macromedia Flash environment, the interface is platform independent. Further, because the final image may be created on a server controlled by a single company, the final image output may be made to have a standardized size and resolution. This enables easy integration with printers, simplifies the production of a personalized product, and simplifies billing on a per-image basis.

By way of example, Figs. 1 and 2 describe the production of a credit card, in accordance with an embodiment of the invention.

In the embodiment of Fig. 1, a customer accesses software according to the invention, after having applied for a credit card through a web site 101 of a card issuer (such as a bank). In the first step, the card issuer issues the customer with a unique identifying number 103 which is passed to an image compilation server 108, which may (or may not) be operated by a company other than the card issuer. The card issuer associates the unique customer identifier 103 with the customer's financial information 104. This association may be performed in a financial account

association table 124 maintained in an environment that is secure from the user interface. The associated customer identifier 103 and financial information 104 are passed to a bank (or other card issuer) printer server 109 via a firewall 102. Next, the customer enters the front end software 105, which may be operated by a website server or other front end server. The customer chooses an image 107 – in Fig. 1, from the customer's computer hard drive 106, and uploads it to the image compilation server 108. The image 107 could come from any suitable source such as an image library maintained by an operator of the image compilation server 108. Back end software 110, running on the image compilation server 108, now enters the original image into a database and generates a web-friendly smaller copy 111 to send to the front end software 105. The customer now performs image manipulations 112 (such as resizing, rotating, and placing the image), as the customer desires. The back end software 110 associates the customer image selection, and subsequent manipulations and selections, with the unique customer identifier 103. Next, the customer chooses another image 113 to overlay on top of the first image 107, and positions image 113 as desired. The overlay image 113 may, for example, be a transparent decorative frame for the uploaded image 107, and may be maintained in an image server 114. The back end software 110 transmits a web-friendly, smaller version 115 of the overlay image 113 to the customer, for use in a creating a combination 116 of the original manipulated image 107 with the overlay image 113. Once customer approval 117 of the final design 116 is achieved and indicated to the front end software 105, the front end software 105 transmits a string of user manipulation data 118 to the image compilation server 108. This string 118 encapsulates the customer's image selections and manipulations. On receiving this string 118 the back end software 110 accesses the original copies of the images from an image library and performs the exact operations that the customer has chosen in the front end software 105 for the customer's final design. In this way, the back end software 110 emulates the manipulations at the user end according to the information transferred in the text string (also referred to herein as the results script). At this point the back end software 110 can output the resulting image 119 to a printer server 120, which may be performed through a firewall 121. The resulting image 119 and associated customer identifier 103 may then be passed to the bank (or other card issuer) printer server 109, which in turn accesses the financial account association table 124 to obtain the associated secure customer financial information 104. The financial information 104 and resulting image 119 may then be sent to a credit card printer 122, which prints a customized

credit card 123. All of the images that are used by the customer in the front end software 105 are issued via the back end software 110. The only information which passes to the back end software 110 from the front end software 105 (apart for requests for images) is data about how the image in front of the customer appears. This information can easily be encrypted for increased security. The number of images combined in a design is not limited to one or two (such as images 107 and 113) – the script can be easily amended for many more layers. Also, transparent frame image layers need not be selected and manipulated before a non-transparent image layer; the image layers can be designed in any order. Text can also be added to the image through a similar replication. The output image can be sent to any type of machine and thus the possible applications are very wide-ranging: the software can be applied not only to the payment card market, but also for non-payment and telephone cards. In certain embodiments, layers may be employed as templates and/or marks, referred to herein as transparencies. In one embodiment, the final image displayed on a card may be restricted to a selected pre-defined area, such as a "window" on a payment card (or other financial account access means), leaving the rest of the card free to contain functional features of the card, such as a bank logo, a payment card hologram or type indicator (such as, for example, "Visa" or "MasterCard" logos). Alternatively, some image layers may be positioned within such a selected window on the card; while other image layers (such as transparencies) are positioned outside the selected window, but surrounding the functional features of the card (such as the bank logo, payment card hologram, etc.). Also, the bank logo or other financial feature can act as a fixed template, behind which the user can move the image to a desired position.

In the embodiment of Fig. 2, in a first step 231, a customer 251 has applied to a bank (or other card issuer) online for a credit card, or is an existing customer offered the opportunity to make a new card for an existing account. In step 232, the customer clicks a link redirecting the user to a website (which may be operated by a company other than the card issuer) for designing the credit card – arriving with a unique identifier which relates to the customer's account and which will be carried with the customer throughout the customer's time on the site. In step 233, the customer identifier is used to log-in; alternatively, the customer could log-in separately at this point and recollect the customer's identifier. Since the design website uses only the customer identifier to identify the customer, it does not obtain any of the customer's financial details. In step 234, the customer elects to upload an image from the customer's own computer 252, such as

a scanned or photographed image. In step 235, the image is uploaded to an image server, and may be held in a database 253 for convenience. In step 236, the customer enters browser-based image manipulation software 254. In step 237, the image manipulation software requests a series of images in web-friendly formats from an image re-size tool 255, so that the process is fast and quick to use. In step 238, the image re-sizing tool requests the original image from the database 253; in step 239, the original image is returned and re-sized to a web-friendly format and size; and in step 240, a set of web-friendly images is returned to the image manipulation software 254 (these are graphical representations of the original images on which manipulations can be performed). Once the customer has achieved the desired effect by manipulating the series of images required, the associated image manipulation commands are sent 241 to an image manipulation emulator 256. Image manipulation commands can include, for example, rotating, re-sizing, positioning, flipping, scaling, brightness controls, red-eye reduction, opacity levels, and other manipulations. In step 242, the image manipulation emulator 256 then requests the original images from the image server so that the best quality image is used. Upon receiving the images in step 243, the emulator 256 then repeats the completed transformations of the customer and creates an image that emulates the one created online, but that uses the original, higher quality graphics. In step 244, this image, and the associated customer identifier, is sent to the bank's printer 257. The financial data corresponding to the customer identifier is obtained, via a secure connection 258 to the bank (or other card issuer); and the printing process set in motion.

In an embodiment according to the invention that places personalized images onto plastic, credit card-style cards, it is necessary to ensure a very high level of security. Therefore, in circumstances where there are already financial records in place for the user, the architecture receives a unique non-sequential customer identifier, which matches with a set of financial records, from the credit card issuer. This customer identifier is passed through each element of the system and is returned with the generated image file. Thus in a "mail merge"-type operation, the customer's personalized image can be matched up with the customer's financial and personal records, so that the correct image is placed on the card. At no time does either the front end or back end software have any financial information. The customer identifier may be used in an automated log-in process. In this way, the software (both the front end and back end software) can know whether the user is new or not. A returning visitor can thus be presented with images that were uploaded on a previous visit.

The system's architecture comprises two distinct elements, in an embodiment according to the invention. The front end element, the element that the user interacts with, is built in Macromedia Flash. This element allows the user to design a card by manipulating (through scaling, rotating, or performing other manipulations such as those given above) the image uploaded and then overlaying the image with frames that can contain transparent sections. Since Flash does not have "local permissions" on the client machine, as it is a browser-based interface, it is not capable of saving the final design. It therefore sends a string of instructions to the second, serverside element. The second, serverside element may be written in C#, although Java, C, C ++, or any other suitable language would be equally capable. The string of instructions may be sent as a "querystring," i.e. as part of the URL; for example, the string could be formatted as:

(createpage.aspx?here_are_the_string_of_instructions&rotate=90&flip=yes...)

Other methods may also be used for transmitting the user's design manipulations, such as using an HTML style "form," or writing the information to a Cookie and then re-reading the information. Alternatively, the hypertext transfer protocol commands HTTP "POST" and HTTP "GET" may be used to pass data from the user session to the server. HTTP "POST" works in an identical fashion to a standard website form; while HTTP "GET" works by changing the URL. For example, an HTTP "GET" could change a URL, in order to transfer a user's rotation, scaling, and other selections, to read:

http://www.personalcard.net/saveinfo.aspx?rotate=90&flip=no&scale=232&x=232&y=12&y2=343&x2=333 etc.

This list of techniques for transmitting the manipulation results is not intended to be exhaustive. Alternatives and future developed techniques will also be suitable.

The customer identifier may be passed using Session State (the webserver's Session Object) or by passing as part of the "querystring," in accordance with an embodiment of the invention. HTML "forms" could achieve the same ends.

In accordance with an embodiment of the invention, an image can be uploaded as a JPEG, GIF, BitMap, PNG, Tiff etc.; although it will be appreciated that nearly any digital image can be

uploaded or output. From the original uploaded image the system creates four separate versions:

1. A thumbnail version (as a JPEG) – see the interface screenshots, below. The image is approximately 1 to 2k in file size.
2. A larger, but still web-optimized version (this is scaled to allow the image to be expanded to the maximum available by the interface – such as scaling 250% - and still have one-to-one pixel matching (i.e. the image size is width 241 x 250% if possible). This is the image used on screen for the design of the card.
3. A Bitmap image at the same scale as the original image. A Bitmap image may be used, for example, in a system that uses C#, which is a Microsoft language and uses Bitmap as the default image type.
4. The output design, which may be sized in proportion to a credit card. This design could be of any software format that is useful to the printer used, such as BMP (Bitmap) or PNG (Portable Network Graphic).

The original images may be placed into a database once they have been uploaded. In one embodiment, each request for images requires going back to the original version to use; however, this need not be the case, because once another image version has been created (e.g. a thumbnail version), the system can equally store this version so that the processing is reduced (though memory taken would increase). A key benefit of an embodiment according to the invention is that it is not necessary to pass the largest image backwards and forwards across the web from client to server, except for the initial upload of images. Nonetheless, when the final edited design or image is generated, the highest quality image is used.

In an embodiment according to the invention, the user designs, on screen, an image that appears the same physical size as a credit card using the screen resolution of 72 dpi. This is because a computer monitor cannot present images at a higher resolution than this. However, a printer can output at higher resolutions, typically 300 dpi or greater – increasing the quality. Although the front end software uses the low resolution images, the final design is compiled by the back end software using a full scale, bitmap version of the original image uploaded. This may be achieved by using a "virtual canvas" within the back end software that is larger than the design canvas within the front end software. Thus the design being created by the back end software is laid on to a background of greater size than in the front end software (while

maintaining 72 dpi resolution). Thus, if the credit card size in pixels is 241 by 153 then, by laying the image on a "virtual canvas" credit card of, 1050 by 672 at 72 dpi, the resolution can be increased to approximately 300 dpi when the credit card is finally printed (back at 3.3 inch by 2.1 inch). This method ensures that the maximum dpi achievable (to the printer's maximum setting) is output from the back end software, but only the resolution necessary is sent to the front end software. This reduces the memory requirements of the client machine and the Internet traffic. This operation could equally be achieved by changing the resolution of a 72 dpi image to 300 at the original size.

In order to use transparencies, in an embodiment according to the invention, the images containing a transparent layer (usually frames or borders) must be converted into Flash "movies" themselves. This process can be manual, but can also be automated to allow images with transparencies (such as bitmaps or PNG) to be imported into the front end software "on the fly." The back end software can use the original PNG or BMP image to generate the credit card image.

Figs. 3-10 show screens of a credit card design website operated in a series of steps according to an embodiment of the invention. Fig. 3 shows a first screen, with a standard library of images assigned to the particular card issuer that is using the credit card design website, on the left of the screen. Fig. 4 shows a screen allowing users to log in so that they can load new images in to the left hand side library. This can be automated in live versions. In Fig. 5, the upload allows the user to browse his or her own computer for images to upload. Fig. 6 shows a screen with a new library including both the user's images and a set of stock images. In the screen of Fig. 7, by clicking on the thumbnail image on the left hand side, the bigger but still web-optimized image is loaded. At this point it can be scaled, flipped, rotated, or undergo other manipulations; and the card details can be viewed or hidden. In the screen of Fig. 8, frames can then be added. These are Flash (.swf) files that allow transparencies. Again they can be flipped, scaled, rotated, or undergo other manipulations; and the card details can be hidden. In the screen of Fig. 9, by clicking on the red Back Button or on the Step 1 tab, the user can return to a previous screen. At this point the image is shown as "live" but the frame can be seen as well. The screen of Fig. 10 shows the final version of the credit card before it is sent off to the back end software to be created.

In accordance with a further embodiment of the invention, shown in Fig. 12, a bank or other card issuer need not create a unique identifier for a customer, and pass that identifier

through the card issuer's own system. Given the complexity of banking systems, avoiding the need to create such an identifier can be an advantage.

Before illustrating the alternative of Fig. 12, Fig. 11 first illustrates an embodiment that may be useful for some card issuers, in which a unique identifier is created for each customer. In this embodiment, a unique identifier is created for each customer that requests to design a card 1101, and passed 1102 to the back end server 1103. The back end server 1103 creates an image corresponding to the customer's unique identifier; and the card issuer 1104 passes the unique identifier through the card issuer's own system. A bureau 1105 that creates the final card can then make a software call to the back end server 1103 using the unique identifier, so that the account details received from the card issuer 1104 may be associated with the image.

In further detail, the embodiment of Fig. 11 functions as follows. Upon a customer requesting to a card issuer 1104 to design a personalized card 1101, the card issuer 1104 creates a unique identifier and passes the identifier 1102 to the back end server 1103. Once the customer designs the card 1106, the user and corresponding unique identifier are returned 1107 to the card issuer, and the back end server stores 1125 the customer image and unique identifier. The information that the customer has requested a new card is then sent 1108 to the card issuer's systems, along with the unique identifier; and a record and unique identifier for the customer are stored 1109 in the card issuer's systems. The card issuer then passes 1110 the unique identifier to the back end server, to notify it that the new card will potentially be created and embossed. The back end server 1103 and/or card issuer 1104 can then perform an image checking procedure 1111 and 1112, to ensure that the image designed by the customer is acceptable for production. If the image fails the back end server's image checking 1111, the unique identifier and reason for the image's rejection is then sent to the card issuer 1113; and the customer is invited 1114 to redesign the card. Once the image has been accepted, the card issuer converts 1115 the customer's record and unique identifier into an emboss record, which is sent 1116 to the bureau 1105 that will be creating the card. The back end server tags the image 1117 to be sent to the bureau 1105 in the next batch of images; and, when a suitable number of images are ready, sends 1118 the image and associated unique identifier to the bureau 1105. The bureau 1105 next stores 1119 the customer's emboss record and unique identifier, obtained from the card issuer 1104; and also stores 1120 the unique identifier and image, obtained from the back end server 1103. Having done so, the bureau 1105 can now create the finished card, by first obtaining 1121 the

customer's record provided by the card issuer 1104; and also using 1122 the unique identifier to obtain the associated customer image and provide it to a blank card stock printer. The blank stock printer may then print 1123 the image onto blank stock, and encode the card's magnetic strip. Based on information in the magnetic strip, the emboss record and printed card stock may then be joined together 1124 to create a finished card.

By contrast with the process of Fig. 11, the embodiment of Fig. 12 allows a card issuer to avoid the need to create for each customer a unique identifier that must be passed through the card issuer's system. Instead, the card issuer creates a "hash value," such as a message digest, or other one-way code, based on some account details for each individual, so that the card issuer can pass customers' account information to the back end server in a way that is completely safe. Referring to Fig. 12, the process is similar to that of Fig. 11, with a card issuer 1204, a back end server 1203, and bureau 1205 performing analogous steps (1201 and following) to those of Fig. 11 (1101 and following). However, a principal difference is found in steps 1202, 1207, 1210, 1213, 1226, and 1227 of Fig. 12, in which a "hash value" (or other one-way code) is passed between the card issuer 1204 and the back end server 1203, instead of requiring the card issuer to create a unique identifier for each customer, as in Fig. 11. First, in step 1202, a hash of a unique part of the customer record (such as the customer's name) is created. A one-way hash, such as the MD5 hash, is a process that takes arbitrary-sized input data (such as a customer's name and account number), and generates a fixed-size output, called a hash (or hash value). A hash has the following properties: (i) it should be computationally infeasible to find another input string that will generate the same hash value; and (ii) the hash does not reveal anything about the input that was used to generate it. This means that the hash function used in the embodiment of Fig. 12 allows the card issuer 1204 to pass at least some of a customer's account information to the back end server 1203 in a way that is completely secure. As seen in steps 1202, 1207, 1210, 1213, 1226, and 1227, a hash value may be passed back and forth between the card issuer 1204 and the back end server 1203, without the need for the card issuer 1204 to create a unique identifier and pass it through its system.

In further detail, the embodiment of Fig. 12 functions as follows. Upon a customer requesting to a card issuer 1204 to design a personalized card 1201, the card issuer 1204 creates a hash value of a unique part of the customer's record 1202 and passes the hash value 1226 to the back end server 1203. Once the customer designs the card 1206, the user and corresponding hash

value are returned 1207 to the card issuer, and the back end server stores 1225 the customer image and hash value. The information that the customer has requested a new card is then sent 1208 to the card issuer's systems; and a record for the customer is stored 1209 in the card issuer's systems. The card issuer then recreates 1210 the hash value that is based on the unique part of the customer record, and passes it 1227 to the back end server 1203, to notify it that the new card will potentially be created and embossed. The back end server 1203 and/or card issuer 1204 can then perform an image checking procedure 1211 and 1212, to ensure that the image designed by the customer is acceptable for production. If the image fails the back end server's image checking 1211, the hash value and reason for the image's rejection is then sent to the card issuer 1213; and the customer is invited 1214 to redesign the card. Once the image has been accepted, the card issuer converts 1215 the customer's record into an emboss record, which is sent 1216 to the bureau 1205 that will be creating the card. The back end server tags the image 1217 to be sent to the bureau 1205 in the next batch of images; and, when a suitable number of images are ready, sends 1218 the image and associated hash value to the bureau 1205. The bureau 1205 next stores 1219 the customer's emboss record, obtained from the card issuer 1204; and also stores 1220 the hash value and image, obtained from the back end server 1203. Having done so, the bureau 1205 can now create the finished card, by first obtaining 1221 the customer's record provided by the card issuer 1204; and also using 1222 the hash value to obtain the associated customer image and provide it to a blank card stock printer. The blank stock printer may then print 1223 the image onto blank stock, and encode the card's magnetic strip. Based on information in the magnetic strip, the emboss record and printed card stock may then be joined together 1224 to create a finished card.

In an alternative to the embodiment of Figs. 11 and 12, which utilize a unique identifier and a hash value, respectively, other methods of creating a secure user identifier may be used. For example, it is also possible for the user information to be encrypted at the card issuer at the beginning of the process, and decrypted at the card bureau using a Private/Public Key or a Private/Private Key encryption technology. This alternative works in a manner similar to the process described in Fig. 12, but with modified security measures; for example, the key must be held by the card bureau.

In another embodiment according to the invention, a secure identifier of the image that is produced based on the user's instructions, may be embedded in the image itself, or embedded as

part of the data file in which the image is stored. For example, a hash key, encrypted identifier, or other secure identifier may be passed through the back end server (such as server 1103 or 1203) in association with the user's image manipulation instructions. At any point in the back end server process, such as when the image is produced for sending to a card bureau (such as card bureau 1205), the image then can be made to have the secure identifier embedded in it – such as by embedding a bar code or other machine-readable code, which encodes the secure identifier, placed in the image itself. In this way, the card bureau 1205 can read the bar code, or other embedded secure identifier, directly from the image itself; and need not acquire any information from the back end server 1203 except for the image itself, which includes the bar code. This embodiment finds particular use in the case where the card production process of the bureau 1205 involves using an image printer, which is not capable of separately storing or passing on the secure identifier. Thus, by using the embedded secure identifier, the image printer can effectively pass on the secure identifier as well as the image to the embossing stage, simply by passing on the printed image itself, which will include the bar code (or other embedded machine-readable identifier). The embossing stage can then involve reading the bar code (or other embedded machine-readable identifier) from the image, and looking up the associated emboss record for use in final card production. It should be noted that the image printing function of bureau 1205 need not be performed within a single organization or enterprise; for example, the image printing may instead be performed by a separate enterprise or department from the organization that performs the embossing, in accordance with an embodiment of the invention. It will be appreciated that a variety of different techniques can be used for embedding the secure identifier in the image, such as by including the identifier in the metadata of the image file; including both when the image file is transmitted to the bureau 1205, or when the image file is in use by the back end server or the bureau.

In another embodiment according to the invention, shown in Fig. 13, a modified architecture may be used, in the context of a card-issuing kiosk or in-store "instant issue" system. As with embodiments described above, front end software runs on a client-side browser; and back end software runs on a remote webserver. However, unlike in the above embodiments, the card printer is located on the client machine (such as a card-issuing kiosk). With reference to Fig. 13, a user browser housed in an in-store kiosk 1302 uses the front end software, which is provided from an internet server 1301, to allow a customer to design a personalized card. The

user's image preferences are then saved and the image is generated 1303 on the remote webserver. The image can then be returned to the kiosk 1304, and printed to the customer's card 1305. Images may be checked on the remote server side, to ensure that they are suitable for printing, in real time, if required. Otherwise the operation of the system may be similar to the embodiments described above.

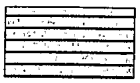
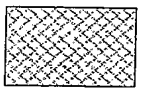
In a further embodiment according to the invention, shown in Fig. 14, a database can be used to store information between the user's image selections, and the back end image production. In this way, the system can be made more scalable, since it does not need to create the images on the back end in real time. As with the other embodiments, the user first makes image selections on the front end interface software, and the image manipulations are passed to the back end server 1401. Then, however, each user's manipulations are saved to a database 1402; so that the back end software can pick up each manipulation, not in real time, and make the high resolution image 1403.

While the foregoing has described what is considered to be the best mode and, where appropriate, other modes of performing the invention, the invention should not be limited to specific apparatus configurations or method steps disclosed in this description of the preferred embodiment. Those skilled in the art will also recognize that the invention has a broad range of applications, and that the embodiments admit of a wide range of modifications without departing from the inventive concepts.

296174

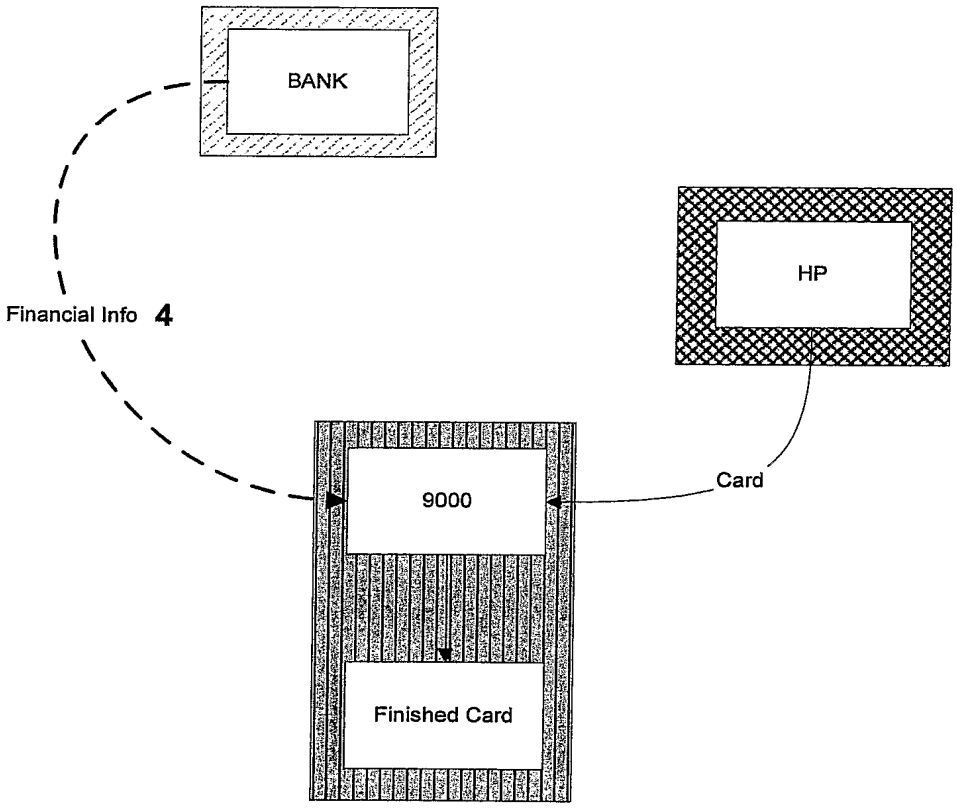
KEY

DRAWINGS PAGE1

BANK	• A Card issuer, it's web presence and other systems
SSG Website	• Serverside Graphics' online presence
SSG Warehouse	• Serverside Graphics' near-line Image storage facility
SSG Print Server	• Serverside Graphics' offline short-term image storage facility - designed to optimize images for the associated printer
HP	• HP Indigo Printer or similar and associated systems
Read / Write	• An optical ID reader and a magnetic stripe writer
9000	• Datacard 9000 or similar card personalization unit
Encryption module	• One-way encryption machine - takes unique secure information and encodes it in a non-reversible fashion
Artista	• A digital printer used to place an image on a card at time of personalization
——DID——→	• Unique, non-sequential Digital ID
——Success DIDs——→	• Digital ID's that relate to successful sessions and have have had the design accepted
——Issue DIDs——→	• Digital IDs that relate to credit approved or re-issue cards to be printed
——OID——→	• Optical ID (Barcode, Microdot, Invisible ink etc.) a method of implanting an ID in the image to be printed on a card
— —Financial info →	• Cardholder details (carried securely)
——Card——→	• Printed plastic card
	• Serverside Graphic's hosting facility
	• Card manufacturer facility
	• Card personalization facility
	• Issuer's facility

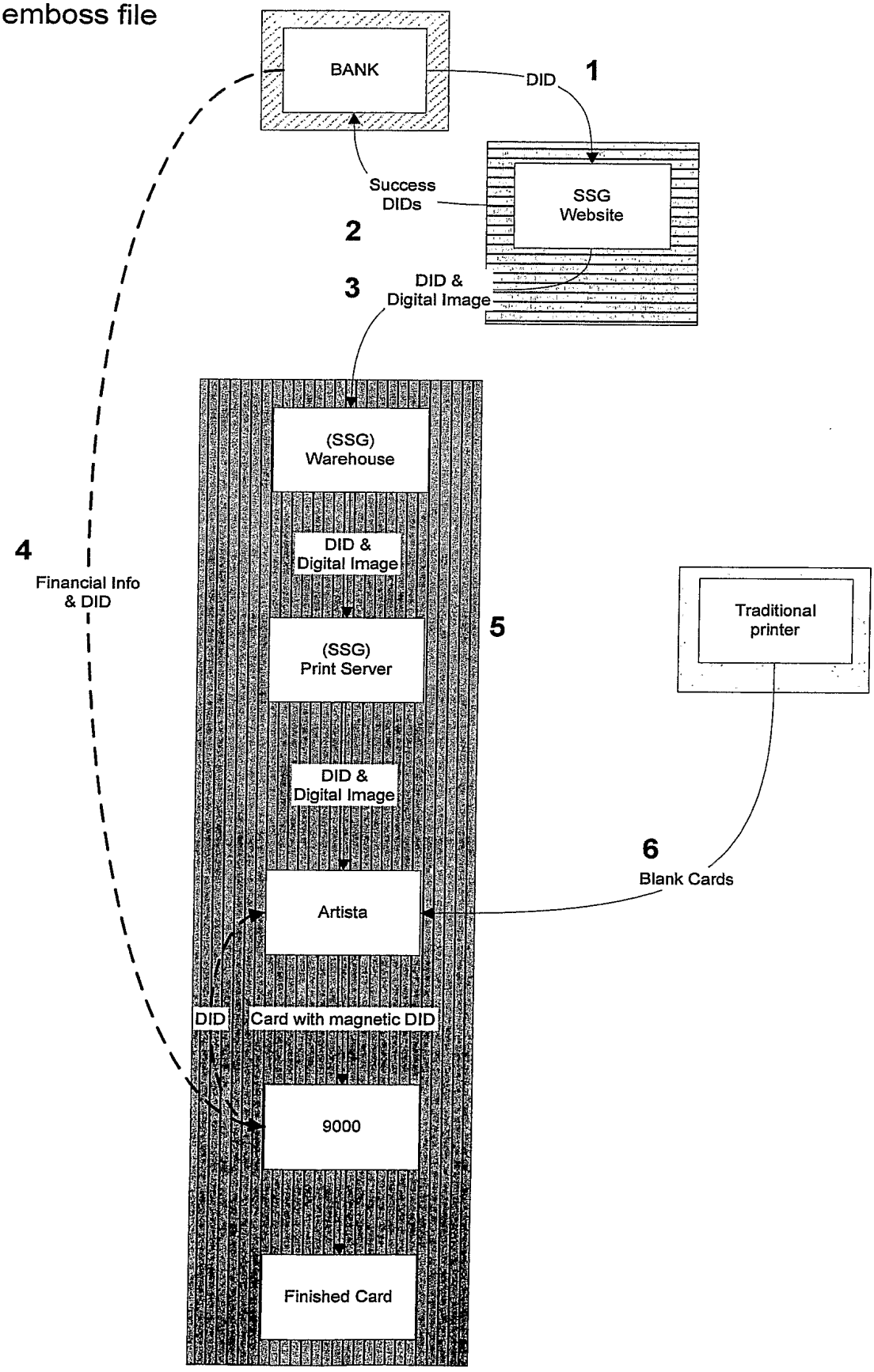
Confidential, Serverside Graphics Proprietary information, Patent Pending

Production without personalisation



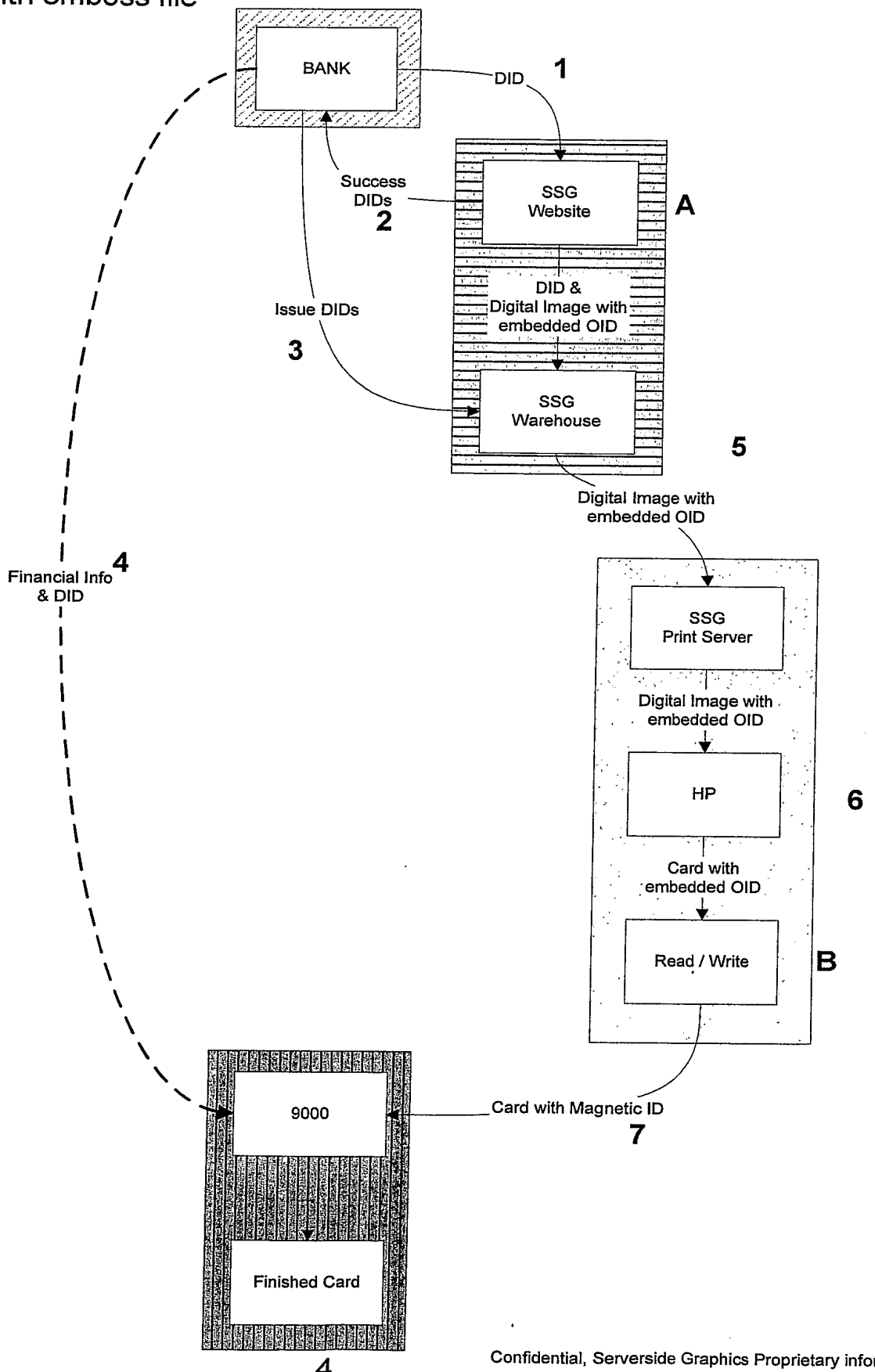
Confidential, Serverside Graphics Proprietary information, Patent Pending

Production using Artista and ID passed with emboss file



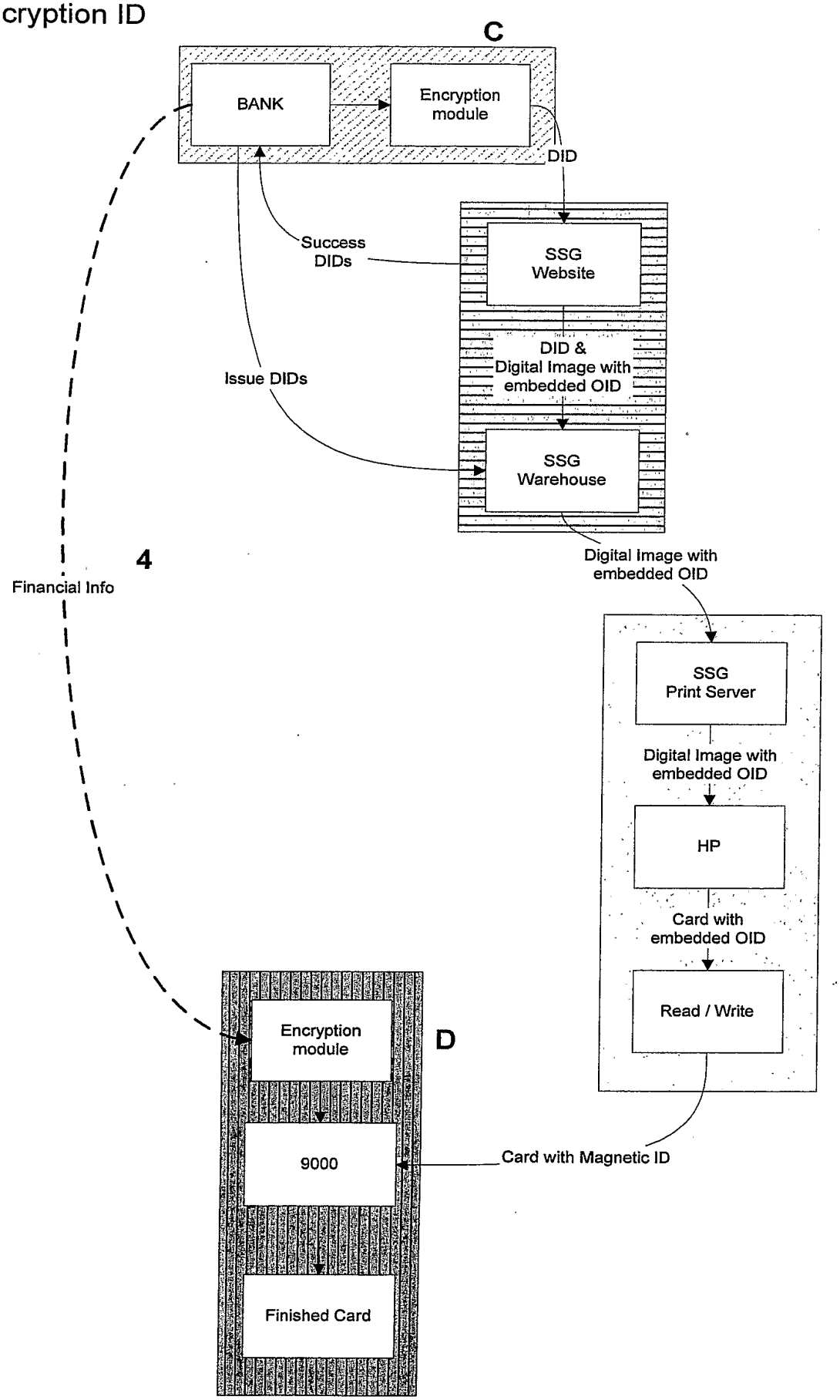
Confidential, Serverside Graphics Proprietary information, Patent Pending

Production using HP and ID passed with emboss file



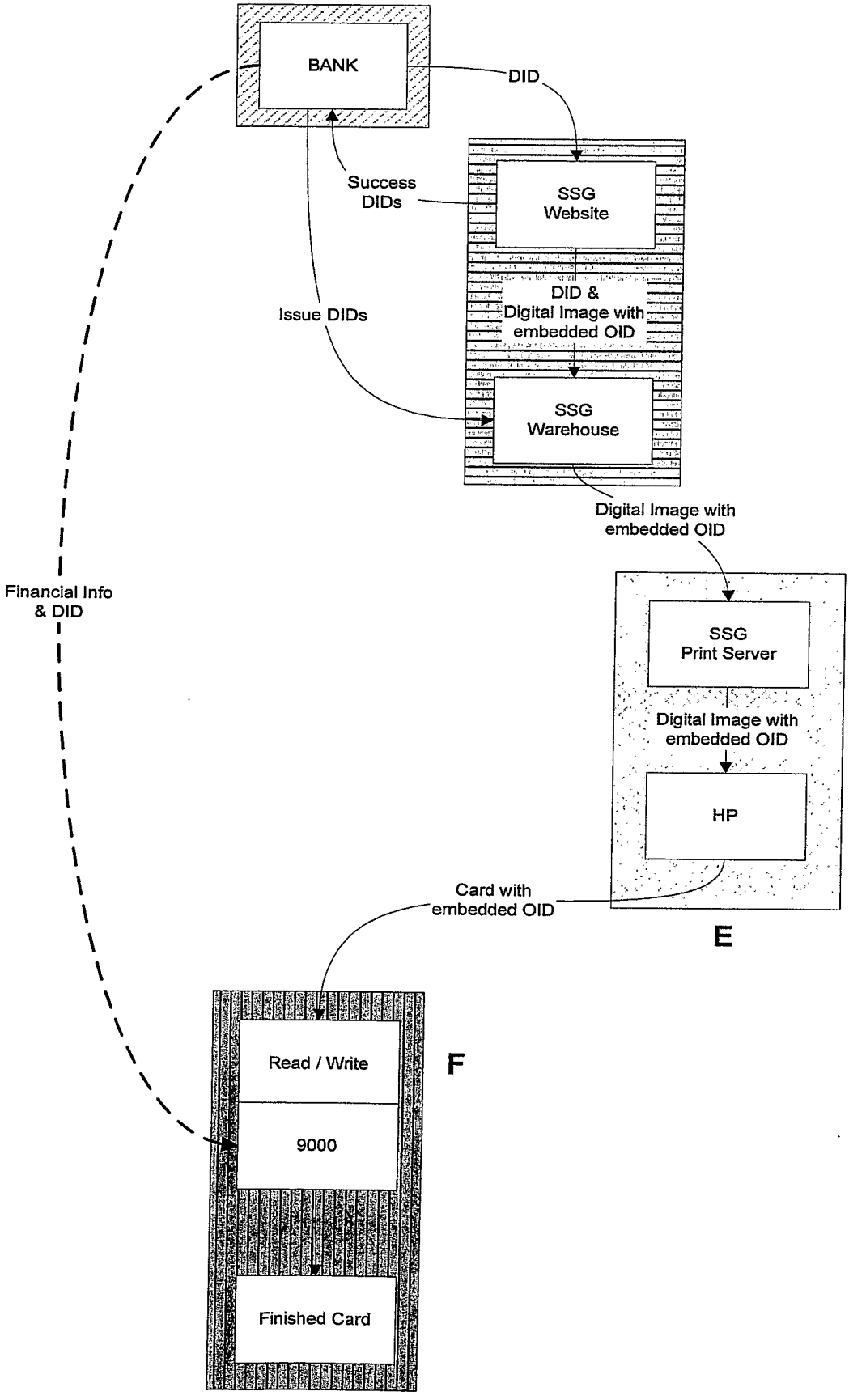
Confidential, Serverside Graphics Proprietary information, Patent Pending

Production using HP and one-way encryption ID



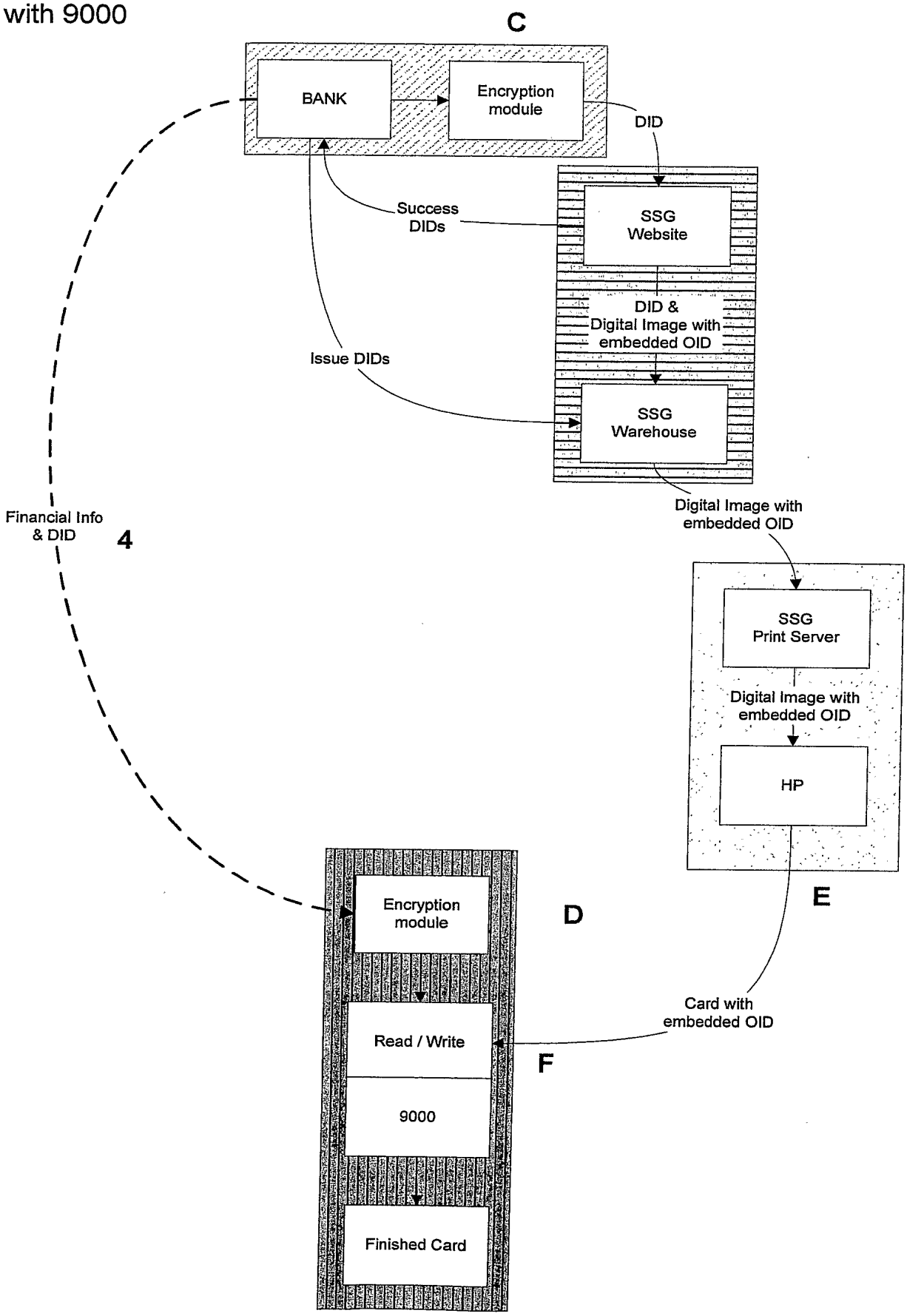
Confidential, Serverside Graphics Proprietary information, Patent Pending

Production using HP and ID passed with emboss file using optical ID compatible with 9000



Confidential, Serverside Graphics Proprietary information,

Production using HP and one-way encryption using optical ID compatible with 9000



Confidential, Serverside Graphics Proprietary information, Patent Pending

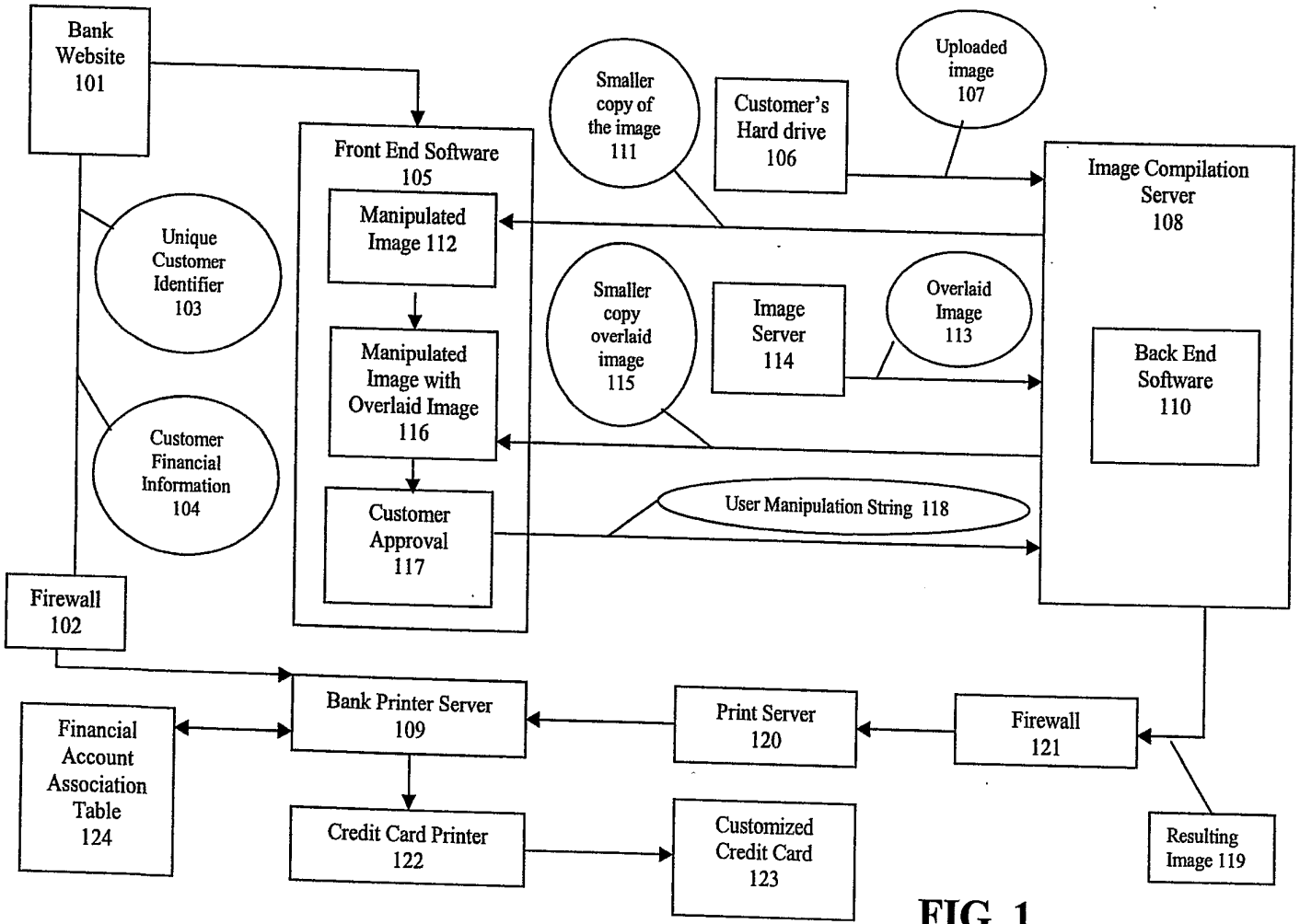

Bank Website 101
Front End Software 105
Manipulated Image 112
Manipulated Image with Overlaid Image 116
Customer Approval 117
Unique Customer Identifier 103
Customer Financial Information 104
Smaller copy of the image 111
Customer's Hard drive 106
Uploaded image 107
Image Compilation Server 108
Back End Software 110
Smaller copy overlaid image 115
Image Server 114
Overlaid Image 113
User Manipulation String 118
Firewall 102
Bank Printer Server 109
Financial Account Association Table 124
Credit Card Printer 122
Customized Credit Card 123
Print Server 120
Firewall 121
Resulting Image 119

FIG. 1

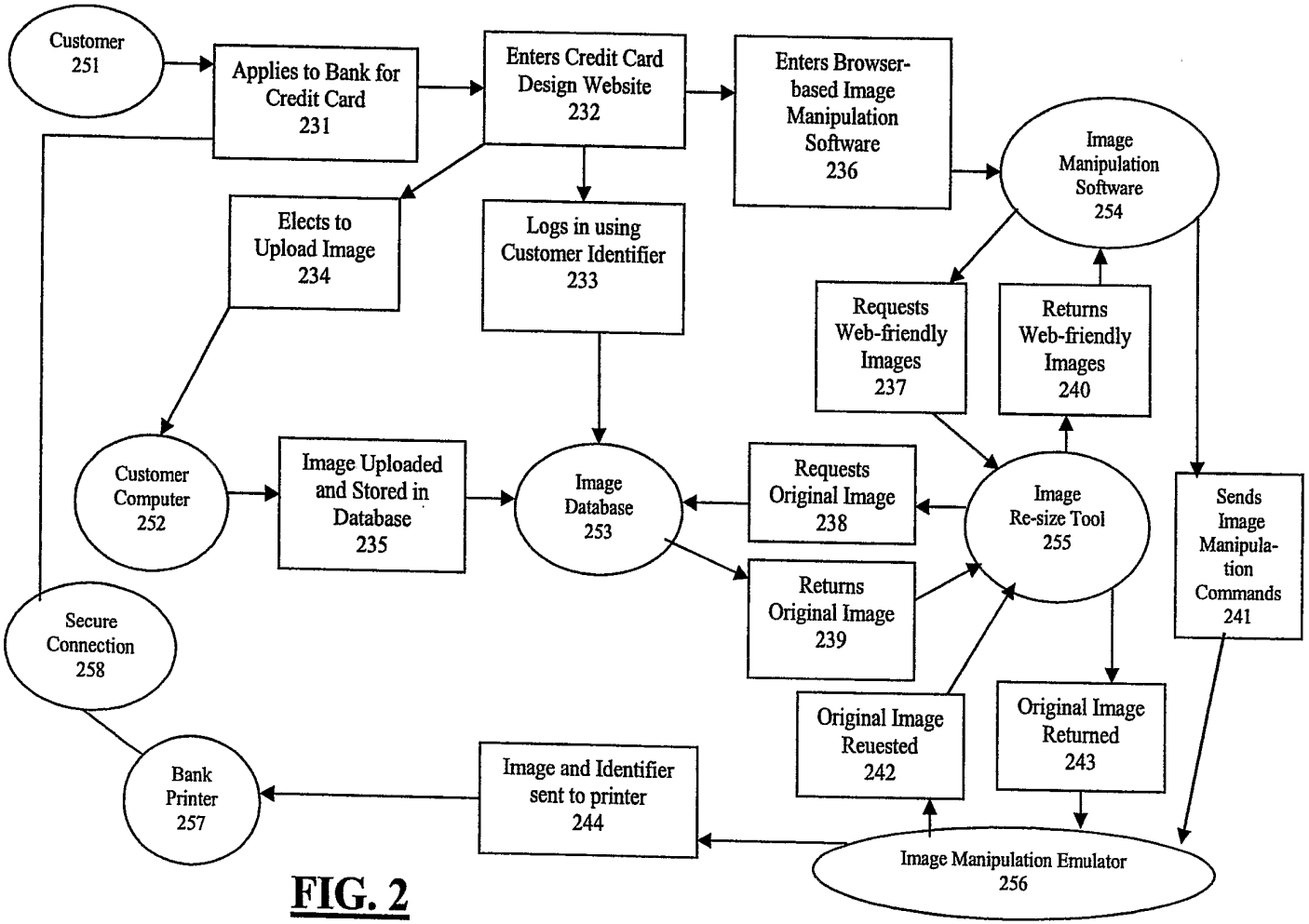

Customer
251
Applies to Bank for Credit Card
231
Enters Credit Card Design Website
232
Enters Browser-based Image Manipulation Software
236
Image Manipulation Software
254
Elects to Upload Image
234
Logs in using Customer Identifier
233
Requests Web-friendly Images
237
Returns Web-friendly Images
240
Customer Computer
252
Image Uploaded and Stored in Database
235
Image Database
253
Requests Original Image
238
Image Re-size Tool
255
Sends Image Manipula-tion Commands
241
Secure Connection
258
Returns Original Image
239
Original Image Reuested
242
Original Image Returned
243
Bank Printer
257
Image and Identifier sent to printer
244
Image Manipulation Emulator
256

FIG. 2

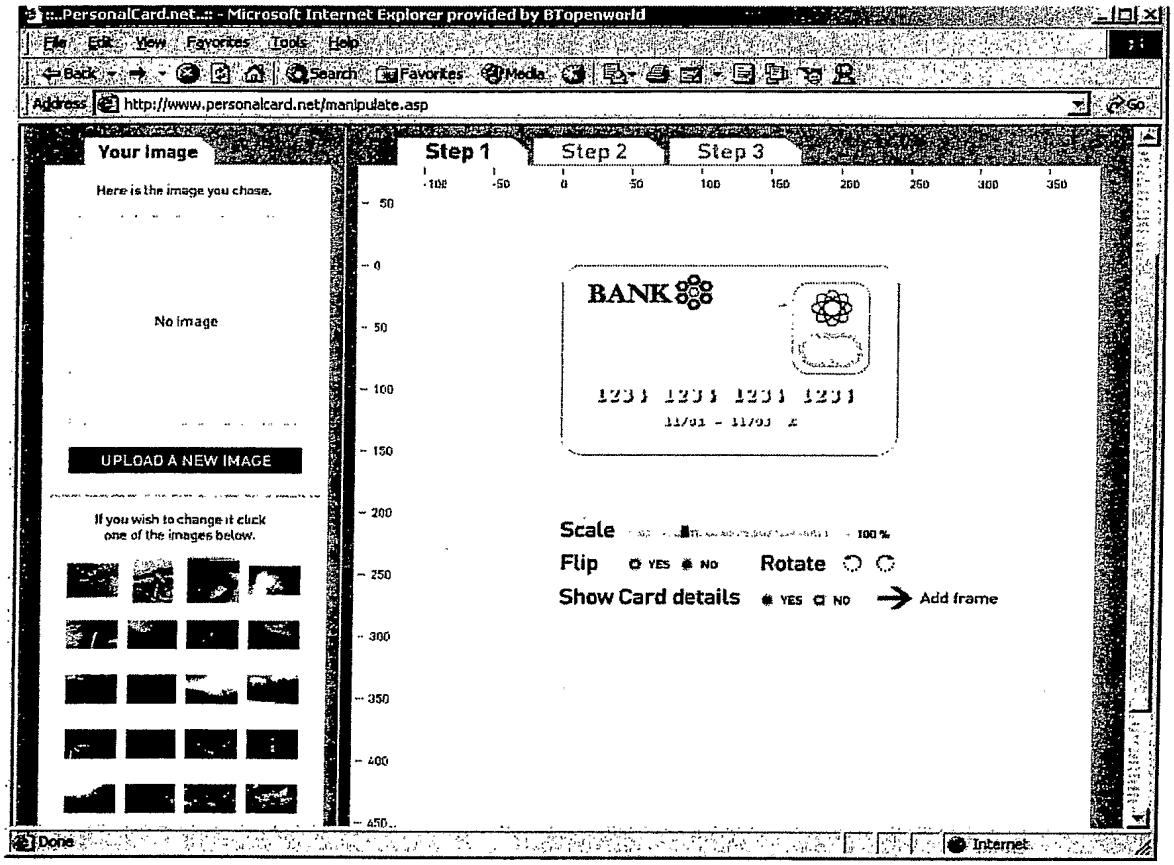

...PersonalCard.net...:: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/manipulate.asp
Your Image
Here is the image you chose.
No image
UPLOAD A NEW IMAGE
If you wish to change it click one of the images below.
Step 1
Step 2
Step 3
BANK
1231 1231 1231 1231
Scale
100 %
Flip YES NO
Rotate
Show Card details YES NO
Add frame
Done
Internet

Fig. 3

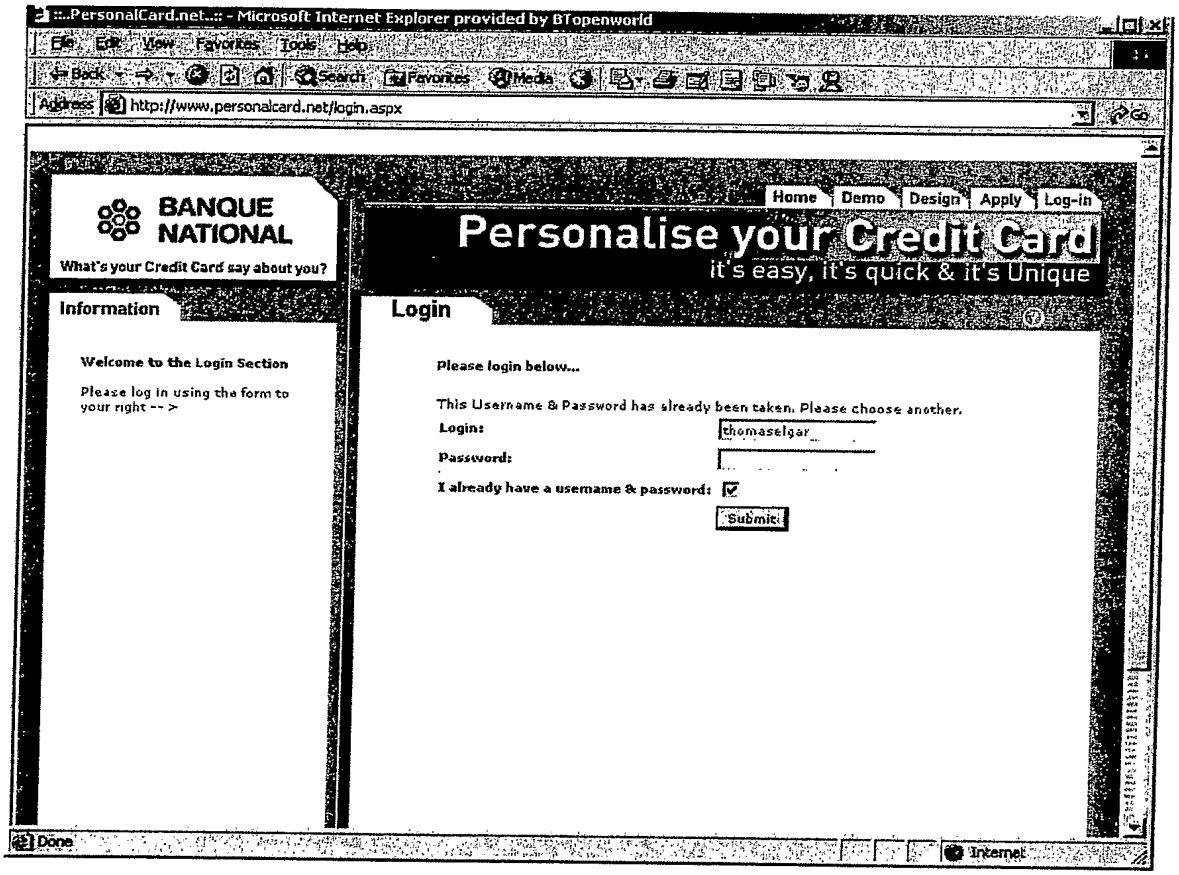

:::PersonalCard.net:::: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/login.aspx
BANQUE NATIONAL
What's your Credit Card say about you?
Home Demo Design Apply Log-in
Personalise your Credit Card
it's easy, it's quick & it's Unique
Information
Welcome to the Login Section
Please log in using the form to your right -- >
Login
Please login below...
This Username & Password has already been taken. Please choose another.
Login: thomaselgar
Password:
I already have a username & password:
Submit
Done
Internet

Fig. 4

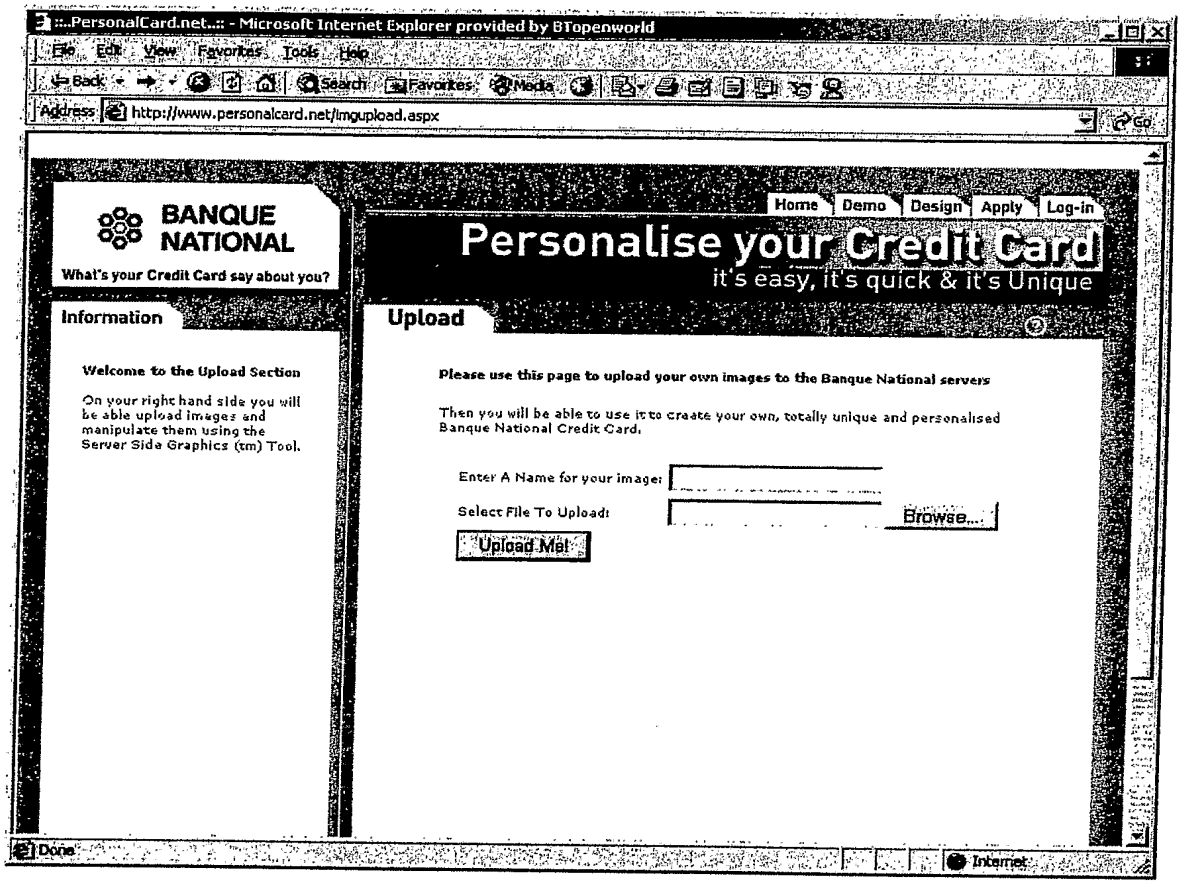

:::PersonalCard.net...:: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/imgupload.aspx
BANQUE NATIONAL
What's your Credit Card say about you?
Home Demo Design Apply Log-in
Personalise your Credit Card
it's easy, it's quick & it's Unique
Information
Welcome to the Upload Section
On your right hand side you will be able upload images and manipulate them using the Server Side Graphics (tm) Tool.
Upload
Please use this page to upload your own images to the Banque National servers
Then you will be able to use it to create your own, totally unique and personalised Banque National Credit Card.
Enter A Name for your image:
Select File To Upload:
Browse...
Upload Me!
Done
Internet

Fig. 5

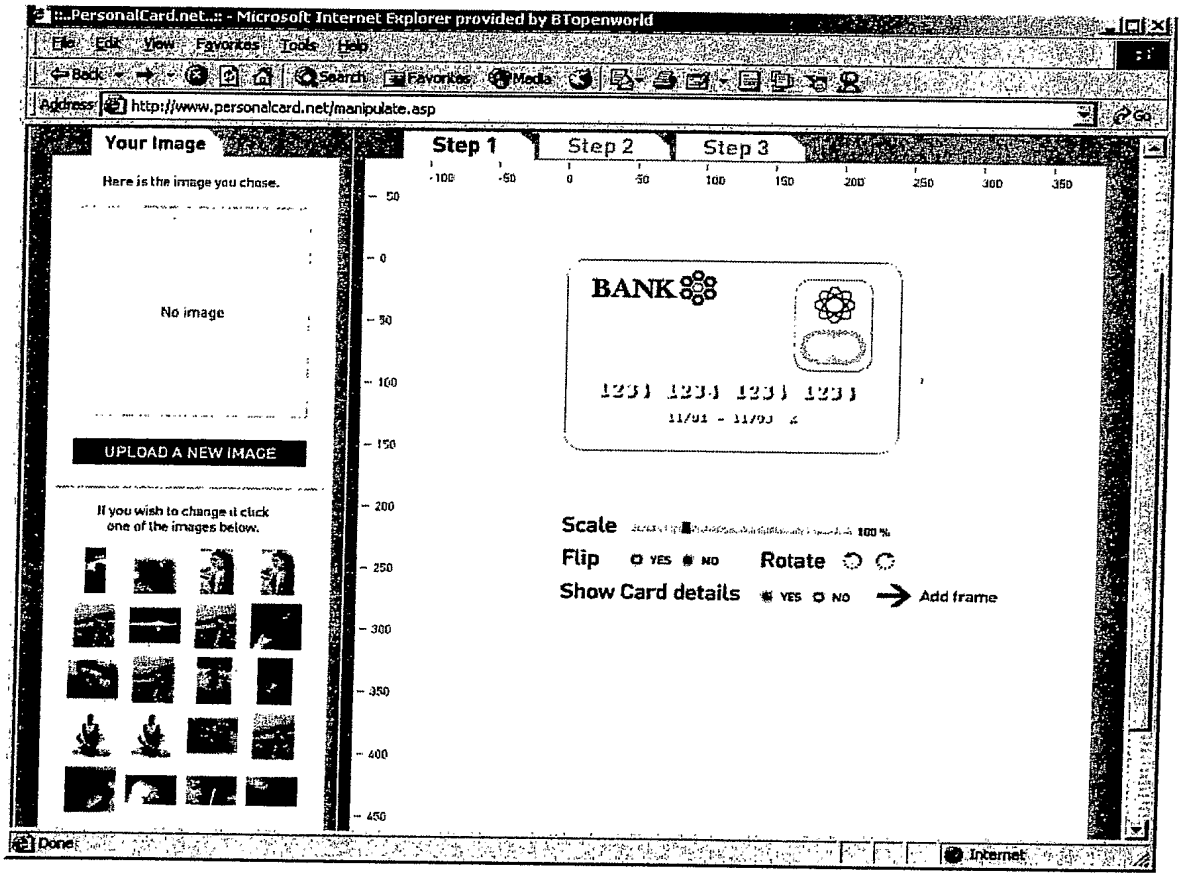

:::PersonalCard.net...:: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/manipulate.asp
Your Image
Here is the image you chose.
No image
UPLOAD A NEW IMAGE
If you wish to change it click one of the images below.
Step 1
Step 2
Step 3
BANK
Scale
Flip YES NO
Rotate
Show Card details YES NO
Add frame
Done
Internet

Fig. 6

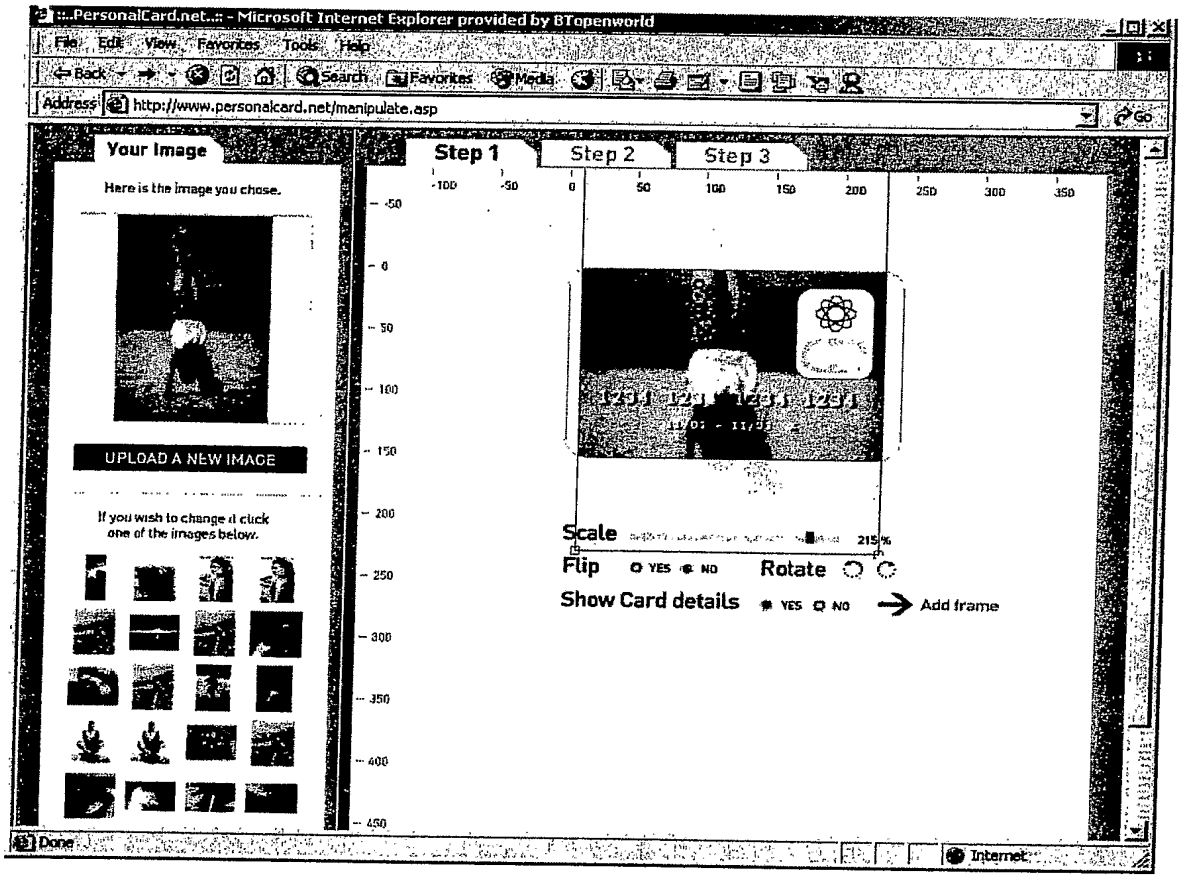

:::PersonalCard.net...:: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/manipulate.asp
Your Image
Here is the image you chose.
UPLOAD A NEW IMAGE
If you wish to change it click one of the images below.
Step 1
Step 2
Step 3
Scale
215%
Flip YES NO
Rotate
Show Card details YES NO
Add frame
Done
Internet

Fig. 7

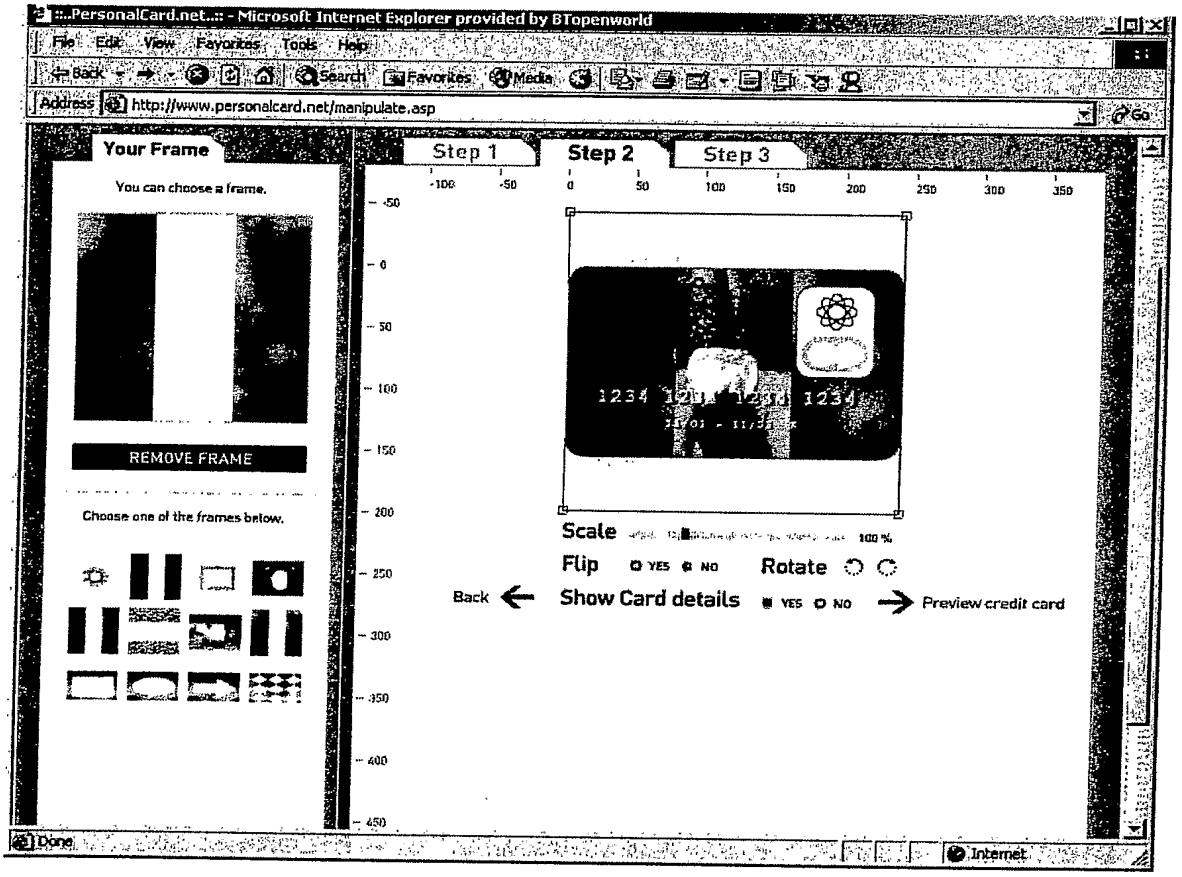

:::PersonalCard.net:::: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/manipulate.asp
Go
Your Frame
You can choose a frame.
REMOVE FRAME
Choose one of the frames below.
Step 1
Step 2
Step 3
Scale
100 %
Flip YES NO
Rotate
Back
Show Card details YES NO
Preview credit card
Done
Internet

Fig. 8

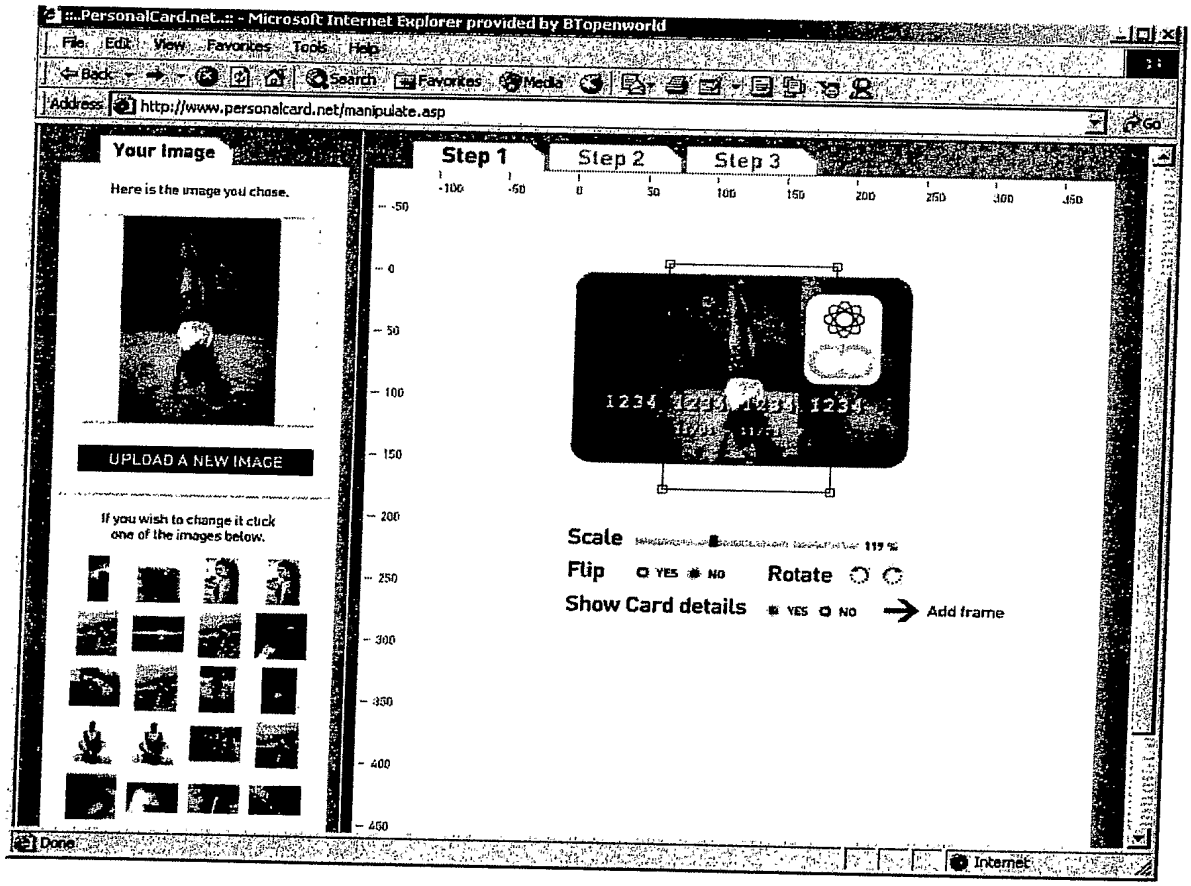

:::PersonalCard.net:::: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/manipulate.asp
Your Image
Here is the image you chose.
UPLOAD A NEW IMAGE
If you wish to change it click one of the images below.
Step 1
Step 2
Step 3
Scale
Flip YES NO
Rotate
Show Card details YES NO
Add frame
Done
Internet

Fig. 9

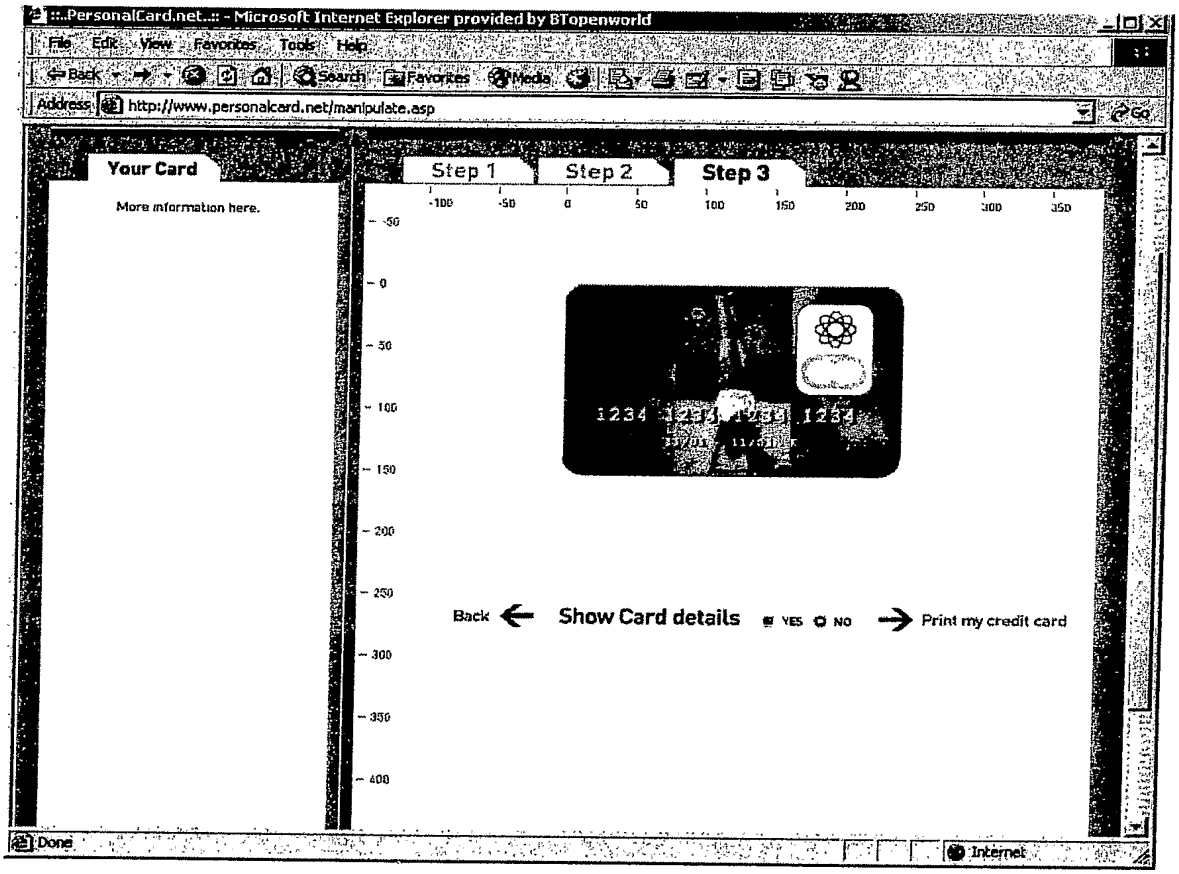

:::PersonalCard.net...:: - Microsoft Internet Explorer provided by BTopenworld
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.personalcard.net/manipulate.asp
Go
Your Card
More information here.
Step 1
Step 2
Step 3
-100 -50 0 50 100 150 200 250 300 350
-50
0
50
100
150
200
250
300
350
400
1234 1234 1234 1234
Back
Show Card details
YES
NO
Print my credit card
Done
Internet

Fig. 10

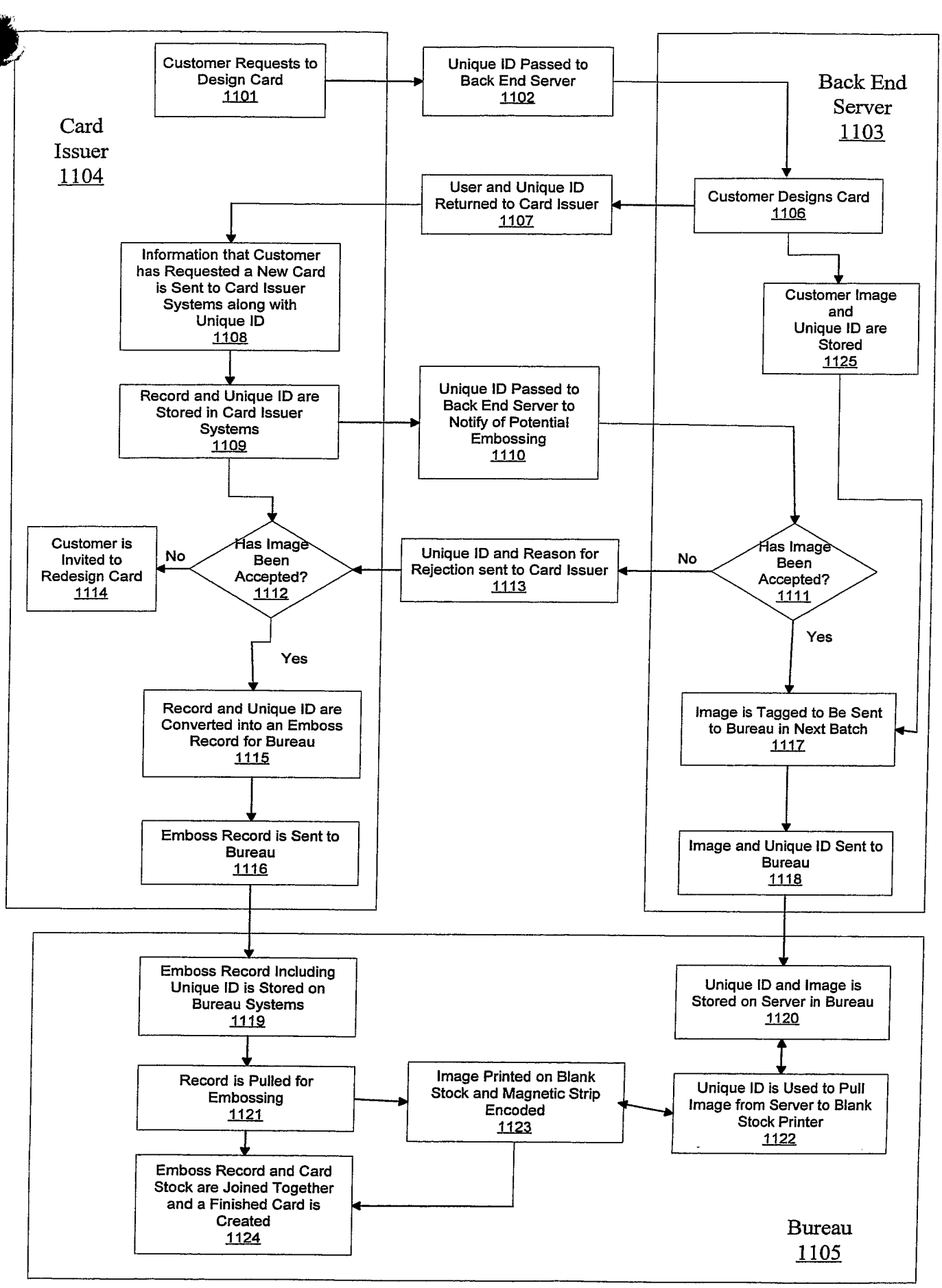

Card Issuer 1104
Back End Server 1103
Bureau 1105
Customer Requests to Design Card 1101
Unique ID Passed to Back End Server 1102
User and Unique ID Returned to Card Issuer 1107
Customer Designs Card 1106
Information that Customer has Requested a New Card is Sent to Card Issuer Systems along with Unique ID 1108
Customer Image and Unique ID are Stored 1125
Record and Unique ID are Stored in Card Issuer Systems 1109
Unique ID Passed to Back End Server to Notify of Potential Embossing 1110
Customer is Invited to Redesign Card 1114
No
Has Image Been Accepted? 1112
Unique ID and Reason for Rejection sent to Card Issuer 1113
No
Has Image Been Accepted? 1111
Yes
Yes
Record and Unique ID are Converted into an Emboss Record for Bureau 1115
Image is Tagged to Be Sent to Bureau in Next Batch 1117
Emboss Record is Sent to Bureau 1116
Image and Unique ID Sent to Bureau 1118
Emboss Record Including Unique ID is Stored on Bureau Systems 1119
Unique ID and Image is Stored on Server in Bureau 1120
Record is Pulled for Embossing 1121
Image Printed on Blank Stock and Magnetic Strip Encoded 1123
Unique ID is Used to Pull Image from Server to Blank Stock Printer 1122
Emboss Record and Card Stock are Joined Together and a Finished Card is Created 1124

Fig. 11

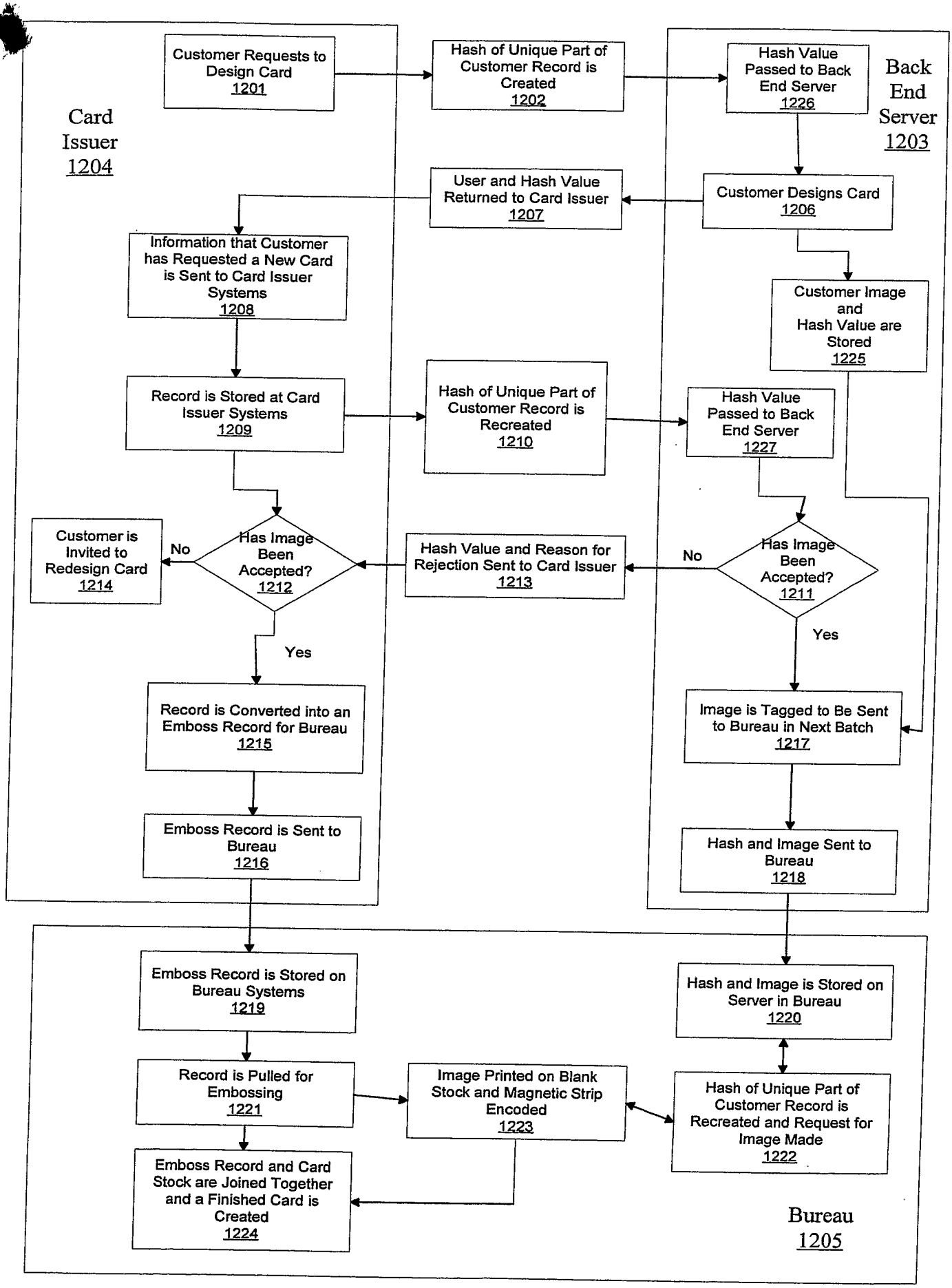

Card Issuer 1204
Back End Server 1203
Bureau 1205
Customer Requests to Design Card 1201
Hash of Unique Part of Customer Record is Created 1202
Hash Value Passed to Back End Server 1226
User and Hash Value Returned to Card Issuer 1207
Customer Designs Card 1206
Information that Customer has Requested a New Card is Sent to Card Issuer Systems 1208
Customer Image and Hash Value are Stored 1225
Record is Stored at Card Issuer Systems 1209
Hash of Unique Part of Customer Record is Recreated 1210
Hash Value Passed to Back End Server 1227
Customer is Invited to Redesign Card 1214
No
Has Image Been Accepted? 1212
Hash Value and Reason for Rejection Sent to Card Issuer 1213
No
Has Image Been Accepted? 1211
Yes
Yes
Record is Converted into an Emboss Record for Bureau 1215
Image is Tagged to Be Sent to Bureau in Next Batch 1217
Emboss Record is Sent to Bureau 1216
Hash and Image Sent to Bureau 1218
Emboss Record is Stored on Bureau Systems 1219
Hash and Image is Stored on Server in Bureau 1220
Record is Pulled for Embossing 1221
Image Printed on Blank Stock and Magnetic Strip Encoded 1223
Hash of Unique Part of Customer Record is Recreated and Request for Image Made 1222
Emboss Record and Card Stock are Joined Together and a Finished Card is Created 1224

Fig. 12

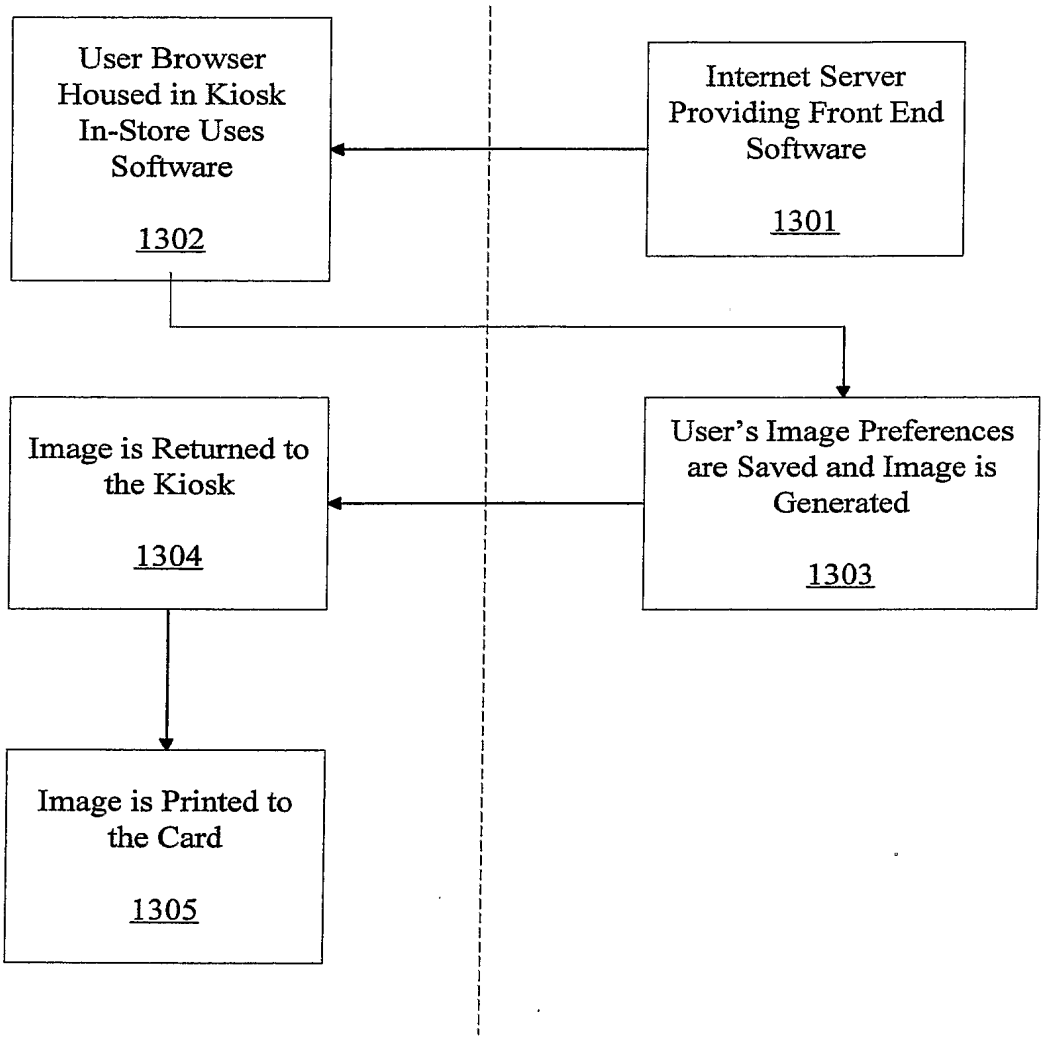

User Browser Housed in Kiosk In-Store Uses Software
1302
Internet Server Providing Front End Software
1301
Image is Returned to the Kiosk
1304
User's Image Preferences are Saved and Image is Generated
1303
Image is Printed to the Card
1305

Fig. 13

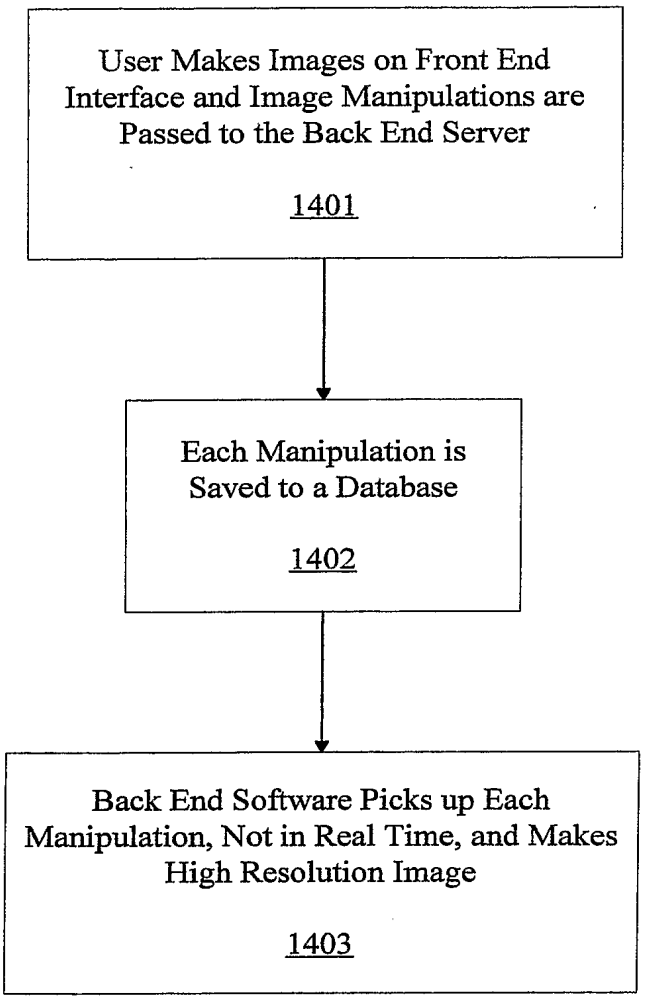

User Makes Images on Front End Interface and Image Manipulations are Passed to the Back End Server
1401
Each Manipulation is Saved to a Database
1402
Back End Software Picks up Each Manipulation, Not in Real Time, and Makes High Resolution Image
1403

Fig. 14

PCT/GB2004/003537